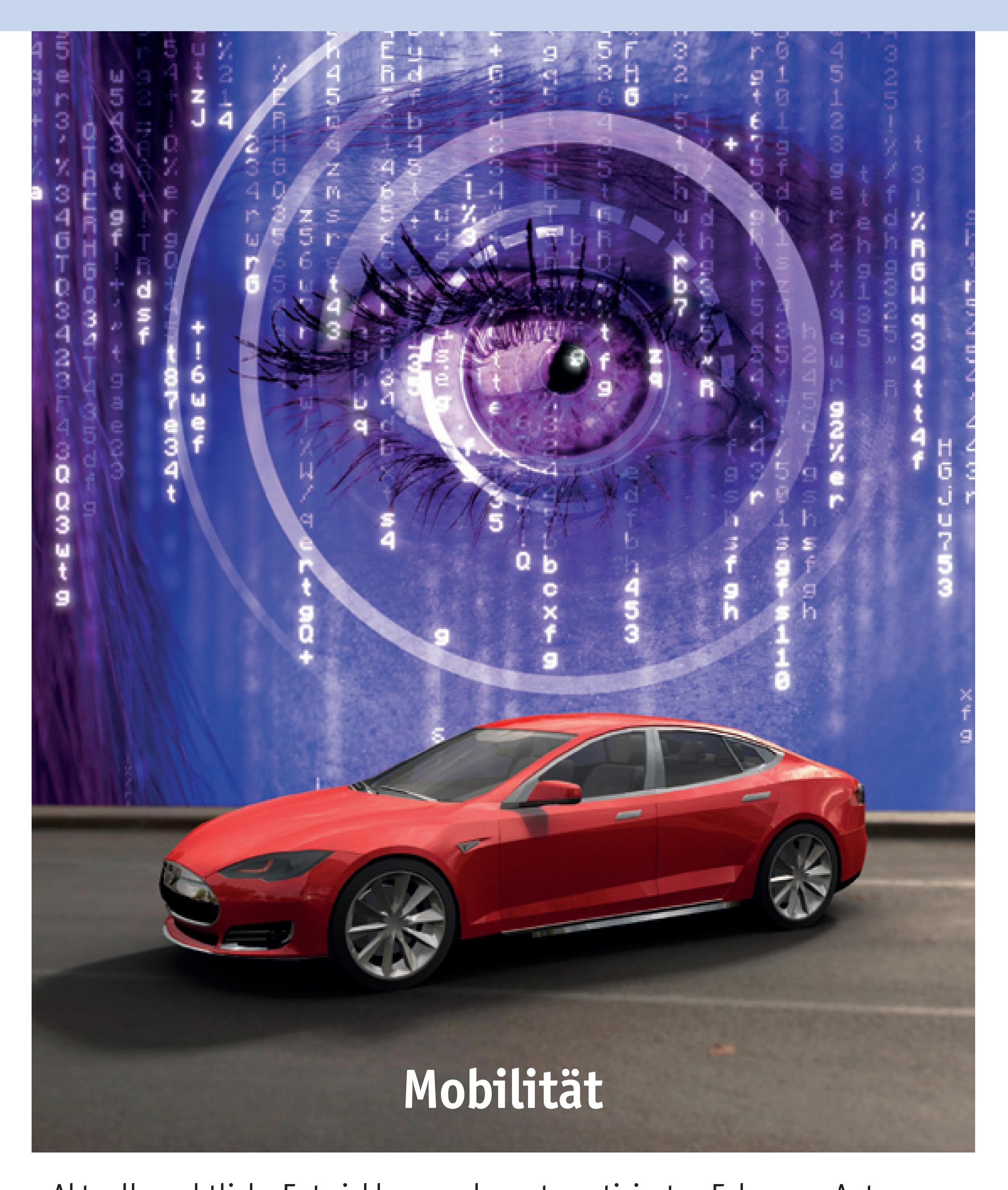
4/2020

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

43. Jahrgang
ISSN 0137-7767
14,00 Euro



Mobilität

■ Aktuelle rechtliche Entwicklungen des automatisierten Fahrens ■ Autonomes Fahren, fliegende Taxis & Co. – Die goldene Zukunft? ■ Tesla – Überwachungsmobil und Datenschleuder ■ Carsharing als Firewall zu den PKW-Herstellern? ■ Datenschutz bei der Nutzung von Mietwagen ■ Moderne Fahrrad-Ausleihe – Ein Erfahrungsbericht ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



27. - 30. Dezember 2020
CCC: rC3 - remote Chaos Experience
Virtuell: https://events.ccc.de/

28. Januar 2021
Europäischer Datenschutztag
In Europa

01. Februar 2021
Redaktionsschluss DANA 1/2021
Schwerpunkt: Biometrie

09. Februar 2021
Safer Internet Day 2021
in Europa

20./21. April 2021
FFD Forum für Datenschutz:
„Datenschutztage 2021 – Der praxis-orientierte Datenschutz-Kongress“
Mainz

23. April 2021
EAID-Tagung „Neue Herausforderungen für die Konzeption von Datenschutz und Informationsfreiheit“
Europäische Akademie Berlin

01. Mai 2021
Redaktionsschluss DANA 2/2021
Schwerpunkt: Bildung

14./15. Juni 2021
Computas: „DuD 2021 - Datenschutz und Datensicherheit“,
23. Jahresfachkonferenz
Berlin

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
43. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Werner Hülsmann
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, iStock, Titel: F. J. Valenta mit Material von clipdealer/ ra2studio und turbosquid.com

Editorial

„Automobil und Internet werden eins“ – so lautet die Überschrift des Interviews des eco-Verbandes der Deutschen Internetwirtschaft mit dem Vorsitzenden des Verbandes der Automobilindustrie Arndt G. Kirchhoff[1]. Hier wird geplant „sämtliche im und am Fahrzeug entstehende Daten“ zu sammeln. Da ein erheblicher Teil dieser Daten einen Personenbezug aufweist, ist die Umsetzung des Datenschutzes ein wichtiger Aspekt bei der Digitalisierung der Mobilität.

Big Data und die sogenannte „künstliche Intelligenz“ bieten Chancen und Risiken bei der künftigen Entwicklung der Mobilität. Neben der Datenschutzthematik sind gerade beim autonomen Fahren weitere Grundrechte betroffen. So geht es hier auch um die Verantwortung für autonome Fahrzeuge, die von selbstlernenden Algorithmen gesteuert werden. Selbst wenn sich die Zahl der Unfälle durch autonomes Fahren verringern sollte – wie von einigen ProtagonistInnen gehofft wird – werden auch autonome Fahrzeuge Unfälle mit Verletzten und Toten verursachen. Da gilt es rechtliche und vor allem ethische Fragestellungen zu beantworten. Daher widmen sich die ersten beiden Beiträge unseres Schwerpunktes „Mobilität“ diesen Themen.

Wie Sie im Beitrag „Tesla – Überwachungsmobil und Datenschleuder“ nachlesen können, scheint es mit dem Datenschutz bei der Entwicklung moderner Fahrzeuge nicht immer so genau genommen zu werden.

Datenschutzthemen gilt es aber nicht nur beim Individualverkehr zu erörtern, sondern auch beim öffentlichen Personennah- und -fernverkehr. So schreibt der VCD Verkehrsclub Deutschland e.V. sehr deutlich: „Das Geschäft mit Nutzerdaten ist ein Markt für sich. Im Bereich Mobilität und der dazugehörigen Infrastruktur wird von Unternehmen eine große Menge personenbezogener Daten hoher Güte generiert. Ortsbezogene Daten machen eine Person in Verbindung mit den Diensten Planung, Ticketing, Zugang, On-Trip-Information etc. transparent.“[2] Auch beim Carsharing sowie der Vermietung von Fahrzeugen aller Art fallen personenbezogene Daten an. Zu letzterem finden Sie ebenfalls zwei Beiträge in diesem Heft.

Sollten Sie sich mit dem Thema vertieft beschäftigen wollen, kann ich Ihnen noch die Dissertation von Florian Sackmann „Datenschutz bei der Digitalisierung der Mobilität“ (siehe Buchbesprechungen) empfehlen.

Nun wünsche ich Ihnen eine interessante Lektüre.

Werner Hülsmann

1 https://www.eco.de/news/automobil-und-internet-werden-eins-interview-mit-arndt-g-kirchhoff/
2 https://www.vcd.org/themen/multimodalitaet/schwerpunktthemen/digitalisierung-mobilitaet/

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied in der DVD, alenfelder@datenschutzverein.de, Köln

Leopold Beer
Jura-Student und freier Journalist, LeopoldBeer@gmx.de

Werner Hülsmann
stellvertretender Vorsitzender der DVD, selbstständiger Datenschutzberater, Ismaning (bei München), huelsmann@datenschutzverein.de

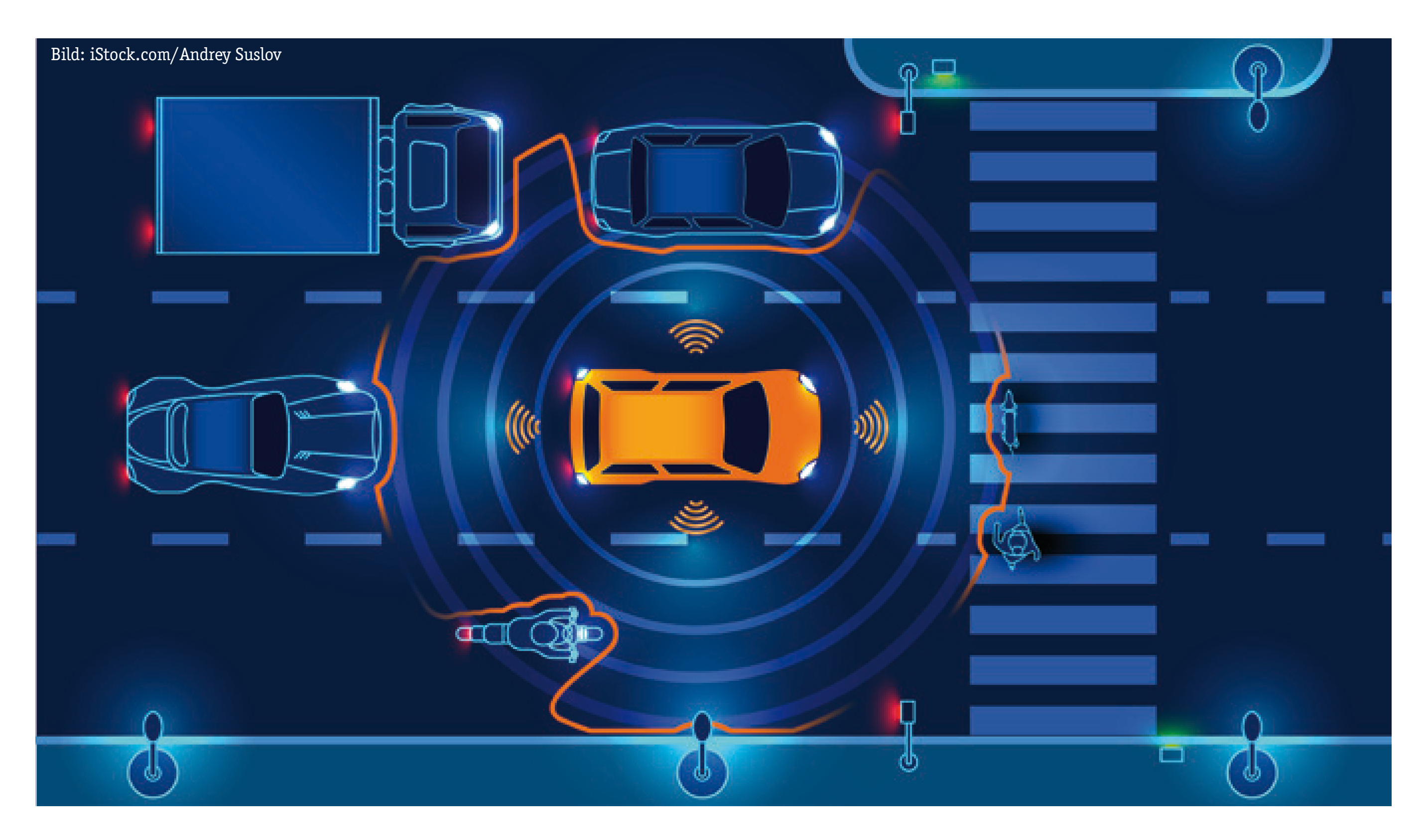
Judith Klink-Straub
Professorin an der Hochschule für öffentliche Verwaltung und Finanzen in Ludwigsburg. Bis Anfang des Jahres war sie Richterin in der Berufungskammer des LG Stuttgart, judith.klink-straub@hs-ludwigsburg.de

Tobias Straub
Professor für Wirtschaftsinformatik an der Dualen Hochschule Baden-Württemberg in Stuttgart sowie behördlicher Datenschutzbeauftragter, tobias.straub@dhbw-stuttgart.de

Thilo Weichert
Vorstandsmitglied in der DVD, Mitglied im Netzwerk Datenschutzexpertise, weichert@datenschutzverein.de, Kiel

Judith Klink-Straub, Tobias Straub

Aktuelle rechtliche Entwicklungen des automatisierten Fahrens


Bild: iStock.com/Andrey Suslov

Deutschland hatte bereits 2017, und damit weltweit als erstes Land, rechtliche Rahmenbedingungen für den Regelbetrieb automatisierter Fahrzeuge der Stufen 3 und 4 (hoch- und vollautomatisiert) verabschiedet. Auf europäischer Ebene sind Länder wie Österreich, Frankreich und die Niederlande mit eigenen Initiativen gefolgt. In den USA wurden in Kalifornien und Arizona sogar schon Vorschriften für das Testen und den Regelbetrieb autonomer Fahrzeuge (der Stufe 5) erlassen.[1]

Dieser Beitrag gibt einen Überblick über die rechtlichen Entwicklungen des automatisierten Fahrens in Deutschland und Europa und diskutiert die Herausforderungen für den Datenschutz.

Regelungen in dem StVG

Für die bereits schon länger verfügbaren Systeme der Stufen 1 und 2 (assistiertes und teilautomatisiertes Fahren) waren noch keine speziellen Regelungen im StVG (Straßenverkehrsgesetz) nötig, da sich hier der Fahrzeugführer ohnehin nicht vom Verkehrsgeschehen abwenden darf. Anders verhält es sich bei den Automatisierungsstufen 3 und 4, auf die sich die vor drei Jahren beschlossenen Änderungen[2] des StVG beziehen.

Konkret wurden neben Anforderungen an das Fahrzeug sowie an das Verhalten des Fahrzeugführers (§§ 1a, b) auch eigene Höchstbeträge für Haftungsfälle, die auf die Verwendung hoch- oder vollautomatisierter Fahrfunktionen zurückgehen, aufgenommen (§ 12 Abs. 1).

Die seit jeher in dem StVG geltende Kombination der Gefährdungshaftung des Halters (gem. § 7 Abs. 1) sowie der Verschuldenshaftung des Fahrers (gem. § 18 Abs. 1) ist für hoch- und vollautomatisierte Fahrzeuge beibehalten worden. § 1a Abs. 4 stellt klar, dass derjenige, der das System zur Fahrzeugsteuerung aktiviert und verwendet, als Fahrzeugführer gilt. Ihm ist ein Entlastungsbeweis bei Nutzung der hoch- oder vollautomatisierten Fahrfunktion möglich, falls nachgewiesen wird, dass keine der folgenden Verhaltensweisen vorgelegen hat:

- nicht bestimmungsgemäße Verwendung der Funktion (§ 1a Abs. 1)
- Nichtbefolgen einer Aufforderung zur Übernahme (§ 1b Abs. 2 Nr. 1)
- Nichterkennen der Notwendigkeit der Übernahme (§ 1b Abs. 2 Nr. 2)

Zur Aufklärung der Frage, ob der Fahrzeugführer diesen Pflichten nachgekommen ist, soll die mit § 63a eingeführte Datenspeicherung beitragen, auf welche unten näher eingegangen wird.

Der in § 1c vorgesehene Bericht des Ministeriums zur Evaluierung der Regelungen steht noch aus, so dass nicht genau absehbar ist, welchen Bedarf es für weitere Anpassungen des StVG gibt.

Entwurf eines Gesetzes zum autonomen Fahren

Auch wenn bis Anfang 2020 noch gar keine Fahrzeuge mit Systemen der Stufen 3 und 4 genehmigt waren,[3] wird aktuell im Verkehrsministerium am (noch nicht öffentlich verfügbaren) Entwurf eines „Gesetzes zum autonomen Fahren in festgelegten Betriebsbereichen" nebst Verordnung gearbeitet, welches allerdings eher auf Mobilitätsanbieter denn Privatnutzer abzuzielen scheint.[4]

Das Verkehrsministerium scheint auch für autonome Fahrzeuge keine Abkehr von der sehr weitreichenden Halterhaftung zu beabsichtigen.[5] Vielmehr sollen auf den Halter deutlich umfassendere Prüf- und Dokumentationspflichten zukommen.

Neu im Entwurf für das autonome Fahren ist dagegen das Konzept eines „Betriebsführers", d.h. einer ständig bereiten natürlichen Person, die jederzeit Fahrmanöver freigeben und das Fahrzeug deaktivieren und in einen risikominimalen Zustand versetzen, jedoch nicht fernsteuern kann.[6]

Der Betriebsführer soll für die Einhaltung der straßenverkehrsrechtlichen Pflichten anstelle des (mit der Automatisierung entfallenden) Fahrzeugführers verantwortlich sein und diesem ausnahmsweise haftungsrechtlich gleichgestellt werden, wenn er vorgeschlagene Manöver freigeben oder das Fahrzeug deaktivieren müsste.[7]

Arten von Fahrzeugdatenspeichern

Sowohl auf nationaler, als auch auf europäischer Ebene gibt es verschiedene Rechtsvorschriften, die eine Pflicht zur Speicherung von Fahrzeugdaten vorsehen. Die Datenerhebung und -verarbeitung bei automatisierten Fahrzeugen wird vor allem damit begründet das Risiko von Verkehrsunfällen zu reduzieren oder diese wenigstens besser aufklären und die Haftungsfrage beantworten zu können.

Bei den im Fahrzeug anfallenden Daten ist in aller Regel ein Personenbezug nach Art. 4 Nr. 1 DSGVO schon dadurch gegeben, dass sie mit der FIN (Fahrzeug-Identifizierungsnummer) oder dem Kfz-Kennzeichen verknüpft und damit dem Halter zuordenbar sind.[8] Insofern wird man, auch schon um Schutzlücken zu vermeiden, die Verarbeitung dem Regime des Datenschutzes unterstellen.[9]

Auf nationaler Ebene sieht § 63a StVG verpflichtend einen *Fahrmodusspeicher* zur Speicherung von Positions- und Zeitangaben vor, zu denen ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und System erfolgt bzw. das System zur Übernahme auffordert.[10] Auch erkannte technische Störungen soll das System in gleicher Weise protokollieren. So soll einerseits verhindert werden, dass sich Fahrer bei einem Unfall pauschal auf ein Versagen des Systems berufen können, andererseits soll die Protokollierung aber auch zur Entkräftung des Schuldvorwurfs beitragen können.[11] Die Daten dürfen dabei an die zur Ahndung von Verkehrsverstößen zuständigen Stellen auf deren Verlangen übermittelt und auch bei diesen gespeichert und genutzt werden (§ 63a Abs. 2 Satz 1 und 2 StVG). § 63a Abs. 3 StVG verpflichtet den Halter unter bestimmten Voraussetzungen eine Datenübermittlung auch an Dritte (wie Unfallbeteiligte) zu veranlassen.[12]

Auf Ebene der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE) wird aktuell auch an einer Standardisierung eines *Data Storage System for Automated Driving* (DSSAD) sowie eines *Event Data Recorder* (EDR) gearbeitet.

Es sei zunächst angemerkt, dass – obwohl EDR häufig als „Unfalldatenspeicher" übersetzt wird – im technischen Sprachgebrauch zwischen einem *Accident Data Recorder* (ADR) und dem EDR differenziert wird. Unter ADR wird dabei ein nachträglich eingebautes Gerät mit eigener Sensorik verstanden, während das EDR (welches häufig mit dem Airbag-Steuersystem kombiniert wird) lediglich Fahrdaten aus den vorhandenen Assistenzsystemen sammelt.[13] Diese Unterscheidung ist zumindest dann datenschutzrechtlich relevant, wenn bei einem ADR noch ein weiterer Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO, etwa der Hersteller des Geräts, an der Datenverarbeitung beteiligt ist.

Die Ansätze DSSAD und EDR sind dabei hinsichtlich Zielrichtung und Verarbeitungslogik klar zu unterscheiden:[14]

- Für das EDR werden eine Vielzahl von Parametern (etwa Geschwindigkeit, Bremsverhalten) kontinuierlich in einem Ringspeicher, dessen Kapazität auf wenige Sekunden beschränkt ist, aufgezeichnet. Ältere Daten werden dabei automatisch überschrieben, sofern nicht ein Ereignis erkannt wird, das auf einen Unfall hindeutet (und z.B. den Airbag auslösen würde).
- Die Speicherung im Rahmen des DSSAD erfolgt dagegen bewusst nicht ereignisgesteuert, sondern lückenlos über einen längeren Zeitraum (im Bereich von Monaten), da die Information, ob ein Mensch oder das System das Fahrzeug gesteuert hat, auch in Situationen (z.B. leichtere Kollisionen, Verstöße gegen Verkehrsregeln) relevant ist, in denen es zu keiner Auslösung des Airbags kommt.

Eine über das kurzzeitige Vorhalten im EDR hinausgehende Speicherung wird schon aufgrund des Umfangs der dabei anfallenden Daten technisch genauso wenig möglich sein, wie eine rein ereignisgesteuerte Aufzeichnung bei DSSAD.[15]

Das DSSAD ist in Konzeption und Zielsetzung dem Fahrmodusspeicher gem. § 63a StVG vergleichbar, während EDRs bislang im deutschen Recht nicht vorgeschrieben sind, aber z.B. in den USA seit langem von den Herstellern verbaut und auf freiwilliger Basis z.B. von Mietwagen-Unternehmen in Deutschland genutzt werden. Fahrer müssen damit rechnen, dass die Auswertung eines Speichers ihres Fahrzeugs bei einem Unfall auch gegen sie verwendet werden kann.[16]

Die Ende vergangenen Jahres verabschiedete EU-Verordnung 2019/2144 gilt ab dem 06.07.2022 mit den in Anhang II festgelegten gestuften Anwendungszeitpunkten für die einzelnen Systeme. Sie sieht insbesondere mit der verpflichtenden *ereignisbezogenen Datenaufzeichnung* einen dem EDR vergleichbaren Fahrzeugdatenspeicher vor, der allerdings im Gegensatz zu diesem und zu DSSDA bewusst so angelegt ist, dass keine personenbezogenen Daten verarbeitet werden (Art. 6 Abs. 5). Der Zweck der Verarbeitung ist auf die abstrakte Unfallforschung und -analyse sowie die Typgenehmigung beschränkt; nur für diese Zwecke dürfen die Daten den nationalen Behörden zur Verfügung gestellt werden (Art. 6 Abs. 4 lit. d).

Daneben schreibt die Verordnung 2019/2144 in Art. 6 Abs. 1 noch sechs



Bild: iStock.com/metamorworks

weitere „hochentwickelte Fahrassistenzsysteme“ vor, darunter eine Vorrichtung zum Einbau einer alkoholempfindlichen Wegfahrsperre und zwei *Warnsysteme* bei *Müdigkeit und nachlassender Aufmerksamkeit* des Fahrers bzw. bei *nachlassender Konzentration*.[17] Für automatisierte und vollautomatisierte Fahrzeuge gelten gem. Art. 11 zusätzliche Anforderungen, insbesondere ist ein System zur *Überwachung der Fahrerverfügbarkeit* vorzusehen. Die konkreten technischen Anforderungen sind von der Kommission aber noch zu präzisieren.

Weniger bekannt dürfte sein, dass für Neuwagen ab dem kommenden Jahr die in *Einrichtungen für die Überwachung des Kraftstoff- und/oder Energieverbrauchs* aufgezeichneten Daten der EU-Kommission bereitzustellen sind. Ziel der Verordnung 2019/631 ist die Reduktion von CO2-Emmissionen und die Schaffung von Transparenz über den tatsächlichen Verbrauch von Fahrzeugen. Art. 12 Abs. 2 sieht dabei vor, dass u.a. die FIN, der Verbrauch und die zurückgelegte Strecke in regelmäßigen Abständen durch Hersteller, nationale Behörden oder aber auch per Direktübertragung zur Verfügung gestellt werden, bevor sie dann anonymisiert und aggregiert weiterverarbeitet werden.

Schon seit März 2018 ist für alle Neuwagen das System *eCall* vorgeschrieben (EU-Verordnung 2015/758), welches bei einem Unfall selbstständig einen Notruf absetzt und dabei einen Minimaldatensatz (wozu insb. die Position, Fahrtrichtung und der Fahrzeugtyp gehören) an die Leitstelle übermittelt. Im Grunde wird dabei für den beabsichtigten Zweck keine Fähigkeit zur Datenspeicherung benötigt, die über die vorigen zwei GPS-Positionen (welche zur Bestimmung der Fahrtrichtung genutzt werden) hinausgeht. Als kritisch wurde bei der Einführung v.a. gesehen, dass eCall (politisch gewollt) den Weg für Zusatzdienste bereiten soll, die personenbezogene Daten der Insassen eines vernetzten Fahrzeugs nutzen.[18]

Neben den gesetzlich vorgeschriebenen und standardisierten Fahrzeugdatenspeichern gibt es herstellerspezifische, die z.T. umfangreichste Datenübermittlungen im Hintergrund veranlassen.[19] Auch in einzelnen Steuergeräten wie jenen des ABS können Daten gespeichert sein, welche sich zur Aufklärung eines Unfalls heranziehen lassen. Sofern Telematik-Tarife genutzt werden, werten zudem Versicherungen laufend Daten über die Fahrweise aus, da diese die Beitragshöhe beeinflusst.

Herausforderungen

Nachdem die Verarbeitung personenbezogener Daten aus dem vernetzten Fahrzeug zunächst eher durch Private wie Hersteller und Versicherungen vorangetrieben wurde, geschieht dies nun mehr und mehr aufgrund gesetzlicher Regelungen. Das Ende der Entwicklung dürfte dabei noch nicht erreicht sein. Wie die Verordnung 2019/631 zeigt, beschränkt sich die Regulierung auch nicht auf automatisierte Fahrzeuge allein.

Während die vom nationalen und europäischen Gesetzgeber beabsichtigten Ziele allgemein wenig umstritten sein dürften, wird zurecht der Datenschutz in den Blick genommen, zumal auch technische Konzepte und Spezifikationen noch fehlen (wie etwa eine Rechtsverordnung gem. § 63b StVG) oder zu große Interpretationsspielräume zulassen.

So ist etwa eine rechtliche Abgrenzung zwischen dem Fahrmodusspeicher gem. § 63a StVG und der in Erarbeitung befindlichen DSSAD-Spezifikation der UNECE noch nicht möglich, wie eine parlamentarische Anfrage ergab.[20] Interessanterweise wird weder von der zuständigen Arbeitsgruppe der UNECE, noch von der Automobilindustrie[21] die Aufzeichnung der Position für das DSSAD als erforderlich angesehen. Angesichts der Sensitivität von Fahrtrouten und der relativ langen Speicherdauer von sechs Monaten für Einträge im Fahrmodusspeicher sollte auch der deutsche Gesetzgeber die Regelung in § 63a StVG überdenken. Sofern nicht gänzlich auf Positionsdaten verzichtet werden soll, wäre es bspw. denkbar diese in verkürzter Form zu speichern, wobei die *führenden* Ziffern der Koordinaten abgeschnitten werden.[22]

Ganz wesentlich für die Bewertung ist die Frage des Orts der Speicherung der im Fahrzeug erhobenen Daten und, damit verbunden, auch die Zugriffsmöglichkeiten. Eine klare Präferenz zur Speicherung inner- oder außerhalb des Fahrzeugs scheint es noch nicht zu geben.[23] Auch wenn der Halter bzw. Fahrzeugführer selbst über den (technischen) Datenzugriff entscheiden kann,[24] wird er hierin nicht völlig frei sein. Die Weigerung, einen von der Versicherung beauftragten Sachverständigen den Fahrzeugspeicher auslesen zu lassen, kann zum Nachteil des Versicherungsnehmers als Verletzung seiner Aufklärungsobliegenheit gewertet werden.[25]

Häufig wird eine Datenspeicherung auf Servern des jeweiligen Fahrzeugherstellers als „natürliche“ Wahl angesehen. Auch wenn technische Gründe dafürsprechen mögen ist jedoch auch die Interessenlage der Hersteller zu bedenken. Z.B. trägt ein Halter bei einem

Produkthaftungsstreit die Beweislast und ist darauf angewiesen, dass der Prozessgegner ihm sämtliche Daten zur Verfügung stellt. Daher ist bereits das Modell eines hoheitlichen Backends für die fahrzeugexterne Datenspeicherung vorgeschlagen worden.[26]

Speziell die Warnsysteme der Verordnung 2019/2144 sind eher „Fahrerüberwachungssysteme“[27] denn Fahrzeugdatenspeicher. Es ist fraglich, wie stark man in diesem Zusammenhang die Datenerfassung einschränken kann, damit diese Systeme noch zuverlässig funktionieren. EG 10 der Verordnung postuliert zwar, dass die Systeme ohne biometrische Daten, einschließlich Gesichtserkennung, auskommen sollten,[28] jedoch verfügen aktuelle Fahrzeugmodelle bereits über Innenraumkameras. [29]

Die im Rahmen der ereignisbezogenen Datenaufzeichnung vorgesehene Anonymisierung ist zu begrüßen. Allerdings gibt es schon Forderungen, dass die Daten dennoch als Beweismittel vor Gericht genutzt werden können.[30] Hier und ebenso bei den anderen Systemen ist also genau darauf zu achten, dass sich nicht doch ein *function creep* einstellt.

Automatisierte und vernetzte Fahrzeuge sind schon treffend als „Smartphones auf Rädern“ oder „rollende Datenbanken“ charakterisiert worden. Offenkundig besteht ein zunehmender Drang zur Sammlung und Verarbeitung personenbezogener Daten aus ganz unterschiedlichen Motivationen heraus. Am Ende darf es nicht zu Verkehrsteilnehmern kommen, die vor Unfallgefahren vermeintlich besser geschützt, dafür aber vollends gläserne Autofahrer sind. Zu erwägen wäre daher ein einheitliches, bereichsspezifisches Regelwerk für alle Verarbeitungen personenbezogener Daten durch Fahrzeuge etwa in der Art der E-Privacy-Verordnung – auch wenn deren bisherige Historie natürlich nicht in jeder Hinsicht als Vorbild dienen kann.

1 Für eine umfassende Darstellung siehe Klink-Straub/Keber, NZV 2020, S. 113 ff.

2 Achtes Gesetz zur Änderung des StVG vom 16.06.2017. Siehe dazu ausführlich Lange, NZV 2017, S. 347 ff.

3 BT- Drucksache 19/17204, S. 2.

4 Handelsblatt, 07.06.2020, https://www.handelsblatt.com/25884018.html.

5 Handelsblatt, Fn. 4.

6 golem.de, 06.10.2020, https://glm.io/151341.

7 Heise Online, 05.10.2020, https://heise.de/-4920962.

8 Lüdemann/Knollmann, ZD 2020, S. 405 f.; Klink-Straub/Straub, NJW 2018, S. 3202, jeweils mwN.

9 Lüdemann/Knollmann, Fn. 8, S. 406.

10 Ausführlich zur Datenverarbeitung im Rahmen von § 63a und der Auswahl des Speicherorts Hoeren/Böckers, JurPC Web-Dok. 21/2020.

11 BT-Drs. 18/11300, S. 24,

12 Klink-Straub/Straub, NJW 2018, S. 3204.

13 Zurlutter: Datenschutzrechtliche Aspekte der Auskunfts- und Aufklärungsobliegenheit über Kfz-Daten in der Kfz-Haftpflichtversicherung, VVW GmbH, 2016, S. 7.

14 Organisation Internationale des Constructeurs d'Automobiles (OICA), Event Data Recorder (EDR) & Data Storage System for Automated Driving (DSSAD), 05.07.2019, https://wiki.unece.org/download/attachments/87621710/EDR-DSSAD-01-04%20%28OICA%29%20Positions%20on%20EDR%20and%20DSSAD.pdf.

15 OICA, Fn. 14, S. 8; auch wird bereits auf die datenschutzrechtliche Problematik einer dauerhaften Aufzeichnung von Fahrzeugdaten wie Videos oder Umgebungsdaten hingewiesen.

16 Z.B. KG Berlin, Urt. v. 06.02.2006 – 12 U 4/04; LG Bochum, Urt. v. 17.10.2016 – I 5 O 291/15.

17 Lüdemann/Knollmann, Fn. 8, S. 405, kritisieren die Trennung der beiden Warnsysteme als unerklärlich und unscharf.

18 Etwa Brink, DANA 1/2015, S. 4.

19 Nürnberger, DuD 2/2018, S.79 ff.

20 BT-Drs. 19/16250, S. 2.

21 IWG on DSSAD, 04.03.2020, http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-06e.pdf, Nr. 8.3.1 sowie OICA, Fn. 14, S. 11.; aA VdTÜV/Dekra/FSD-Zentrale Stelle, Gemeinsame Position zur Ausgestaltung des Fahrmodusspeichers (DSSAD), 02.08.2019, S. 5, https://www.vdtuev.de/dok_view?oid=749911.

22 Dies würde ein Nachvollziehen der gefahrenen Strecken erschweren und dennoch bei einem Vorfall – der sich ja lokalisieren lässt – eine genaue Rekonstruktion der Fahrstrecke direkt am Ort des Geschehens ermöglichen.

23 BT-Drs. 19/16250, S. 3.

24 Brink, Fn. 18, S. 7, bringt sogar einen „Panik-Knopf“ ins Spiel, mit dessen Hilfe der Fahrzeugführer sämtliche Daten löschen kann.

25 LG Köln Urt. v. 26.03.2020 – 24 O 236/19.

26 VdTÜV et al., Fn. 21, S. 1 f.

27 Lüdemann/Knollmann, Fn. 9, S. 404.

28 Vgl. dazu Lüdemann/Knollmann, Fn. 9, S. 405.

29 heise Autos, 28.10.2020, https://heise.de/-4939003.

30 ADAC, Standpunkt Ereignisdatenspeicher, 11.07.2019, https://www.adac.de/-/media/pdf/vek/fachinformationen/automatisieung-und-digitalisierung/event-data-recorder-adac-sp.pdf.

Leopold Beer

Autonomes Fahren, fliegende Taxis & Co. – Die goldene Zukunft?

Eine rechtliche Analyse des Einsatzes von KI im Mobilitätssektor

Immense Fortschritte in der Leistungsfähigkeit von Hard- und Software haben die Technologie weit über die einfache Darstellung und sonstige Verarbeitung von Informationen in elektronischer Form, d.h. die „klassische" Digitalisierung, hinausgeführt. Der Begriff „künstliche Intelligenz" (KI) bezieht sich auf Software, die selbstständig lernt und entscheidet. KI ist in der Lage komplexe Auswahlprozesse mit einer Vielzahl von Daten selbständig durchzuführen und mit Hilfe softwaregesteuerter Maschinen umzusetzen. Während Algorithmen ursprünglich elektronische Selektionsprozesse waren, die von menschlichen Programmierern bestimmt wurden, können Algorithmen der neuen Generation auf der Basis von Strukturen neuronaler Netze mit Rückkopplungsmechanismen aus großen Datenmengen, mit denen sie gefüttert werden, autonom Muster erkennen, Informationen kategorisieren, also „lernen" und selektieren, d.h. entscheiden („maschinelles Lernen"). Die KI ist in der Lage auf der Basis von möglichst umfangreichem Datenmaterial durch Vergleich abstraktes „Denken" zu simulieren. Auf diese Weise löst sich die KI von den Vorgaben der Programmierer und setzt das Megathema der menschlichen Kontrolle über die KI auf die Tagesordnung politischer, ethischer und rechtlicher Diskussionen. Denn nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden.

Insbesondere die Frage des Datenschutzes bei autonomen Systemen ist eine wesentliche Herausforderung. Im Mobilitätssektor kann KI beispielsweise im Rahmen des autonomen Fahrens eingesetzt werden. Hierbei werden massenhaft Daten verarbeitet, die teilweise auch einen Personenbezug vorweisen, sich also nach der Definition der EU-Datenschutz-Grundverordnung (DSGVO) auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Wahrung der Rechte und Freiheiten dieser Personen ist von essenzieller Bedeutung.

Hambacher Erklärung

Als eine Art Wegweiser hinsichtlich des Einsatzes von KI unter Wahrung des Datenschutzes kann die Hambacher Erklärung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 03. April 2019 verstanden werden. Hier setzen die Datenschutzaufsichtsbehörden erste Rahmenbedingungen hinsichtlich des Einsatzes von KI.

Zunächst gelten für KI-Systeme die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO), welche frühzeitig durch technische und organisatorische Maßnahmen vonseiten des Verantwortlichen umgesetzt werden müssen (Privacy by Design). Ergänzend wird von den Datenschutzaufsichtsbehörden in dem Positionspapier gefordert, dass:

a. KI Menschen nicht zum Objekt macht (Art. 1 Abs. 1 GG, Art. 1 GRCh),
b. KI nur für verfassungsrechtlich legitimierte Ziele eingesetzt wird und das Zweckbindungsgebot nicht aufhebt (Art. 5 Abs. 1 lit. b DSGVO),
c. KI transparent, nachvollziehbar und erklärbar ist (Art. 5 Abs. 1 lit. a und 12 DSGVO),
d. KI Diskriminierungen vermeidet (Art. 3 GG, Art. 20 GRCh),
e. KI den Grundsatz der Datenminimierung einhält (Art. 5 Abs. 1 lit. c DGVO),
f. KI die Bestimmung des Verantwortlichen ermöglicht (Art. 5 Abs. 2 DSGVO) und
g. KI durch technische und organisatorische Maßnahmen datenschutzgerecht ausgestaltet wird (Art. 24, 25 und 32 DSGVO).

Use-Case: Autonomes Fahren

Im Folgenden werden datenschutzrechtliche Rahmenbedingungen exemplarisch am Einsatz von KI im Bereich des autonomen Fahrens erläutert. Hier ist zunächst zu prüfen, ob ein Personenbezug der verarbeiteten Daten vorliegt und ob überhaupt von einer Datenverarbeitung im Sinne der DSGVO gesprochen werden kann. Im Anschluss muss der Verantwortliche bestimmt werden, der die Zulässigkeitsvoraussetzungen für eine Verarbeitung erfüllen und die Datensicherheit gewährleisten muss.

Personenbezug

Eine Anwendbarkeit des Datenschutzrechts ist nur dann zu bejahen, wenn ein Personenbezug vorliegt. In Art. 4 Nr. 1 DSGVO sind personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder eine identifizierbare natürliche Person beziehen, definiert. Einige Daten, wie die Positionsdaten des Fahrzeuges, haben in jedem Fall einen Personenbezug zum Fahrer des Kfz. Doch auch Daten über das Umfeld des autonom fahrenden Autos können – je nach technischer Ausgestaltung – als personenbezogene Daten anderer Verkehrsteilnehmer gewertet werden. So ist ein Großteil aller im Rahmen des autonomen Fahrens erhobenen Daten als personenbezogen zu qualifizieren.

Ein spannender Diskussionspunkt ergibt sich aus der Tatsache, dass KI auch in der Lage sein kann, neue Datenquellen zu erschließen und gesammelte Daten damit zu verknüpfen, was den Diskussionsbereich um das Phänomen „Big Data" eröffnet. Problematisch ist hier insbesondere, dass KI in der Lage

sein kann ursprünglich anonyme Daten eines Betroffenen durch Auswertung zusätzlicher Informationsquellen einer Person zuzuordnen. Eine Zulässigkeit dieser Verkettung von Informationen und der Herleitung neuer Daten (beispielsweise durch statistische Zusammenhänge) ist wohl im Einzelfall zu beurteilen.

Datenverarbeitung

Im nächsten Schritt gilt es zu beurteilen, ob überhaupt eine Datenverarbeitung im Sinne der DSGVO vorliegt. Was unter einer Datenverarbeitung zu verstehen ist, wird in Art. 4 Nr. 2 DSGVO legaldefiniert. So ist eine Verarbeitung „jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten". Exemplarisch werden anschließend das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung als relevante Datenverarbeitungsvorgänge genannt.

Zahlreiche Datenverarbeitungsvorgänge im Zusammenhang mit autonomem Fahren dürften nach dieser Definition zweifelsfrei als Datenverarbeitung i.S.d. DSGVO zu beurteilen sein. Schwieriger wird die Einordnung, wenn Daten innerhalb eines Bruchteils von einer Sekunde durch KI ausgewertet und anschließend sofort wieder überschrieben werden, wie das insbesondere beim Einsatz von Ultraschall, Radar und Lidar im Rahmen der Umgebungsüberwachung beim autonomen Fahren üblich ist. Eine Speicherung solcher Daten über den Zeitpunkt der Auswertung durch autonome Systeme hinaus ist in aller Regel nicht erforderlich. Nach Wertung der DSGVO spielt die Dauer des Vorgangs zwar keinerlei Rolle bei der Beurteilung des Vorliegens einer Datenverarbeitung, doch im Einzelfall kann eine differenzierte Betrachtung geboten sein. So ist eine Verarbeitung wohl stets dann zu verneinen, wenn eine Überschreibung der Daten so schnell erfolgt, dass für einen Menschen keinerlei Möglichkeit der Kenntnisnahme besteht. An dieser Stelle ist jedoch zu berücksichtigen, dass diese Ausnahme keine wesentliche Rolle in der Praxis spielen dürfte, da bereits aus Gesichtspunkten der IT-Sicherheit eine Eingriffsmöglichkeit des Menschen bestehen muss.

Verantwortlicher

Die Bestimmung des Verantwortlichen beim autonomen Fahren ist häufig nicht leicht, da eine Vielzahl von Beteiligten mitwirken. Die DSGVO versteht unter dem Verantwortlichen diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Es ist also darauf abzustellen, wer konkret über das Ob, Warum und Wie der Datenverarbeitung entscheidet, also faktisch Einfluss auf die Datenverarbeitung ausübt. Als Verantwortlicher kommen in Betracht der Eigentümer und Halter bei Daten über Fahrer des Fahrzeugs und Mitfahrer (wobei hier das sog. „Haushaltsprivileg" des Art. 2 Abs. 2 lit. c DSGVO zu berücksichtigen ist), der Hersteller bei einer permanenten Datenübertragung oder Bestehen einer Zugriffsmöglichkeit ohne Mitwirkung des Halters auf das Fahrzeug, die Versicherung im Falle einer Übermittlung von Daten über das Fahrverhalten im Zusammenhang mit einem Telematik-Tarif oder Werkstätten bei Auslesung von Daten aus dem Fahrzeug.

Zulässigkeit

Die rechtliche Zulässigkeit von Datenverarbeitungen ist in der DSGVO nach dem Prinzip eines Verbots mit Erlaubnisvorbehalt ausgestaltet. Personenbezogene Daten dürfen demzufolge nur verarbeitet werden, wenn einer der Ausnahmetatbestände des Art. 6 DSGVO erfüllt ist.

Hier ist zunächst Art. 6 Abs. 1 S. 1 lit. c DSGVO heranzuziehen, nach dem eine Verarbeitung dann zulässig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist. Als eine solche rechtliche Verpflichtung kommt insbesondere § 63a Straßenverkehrsgesetz (StVG) in Betracht, der vorsieht, dass in kritischen Situationen die per Satellitennavigationssystem ermittelten Positionsdaten und der Zeitpunkt gespeichert werden, um so Unfälle aufklären sowie Fehlfunktionen nachvollziehen zu können. Diese Daten dürfen gem. § 63 a Abs. 2 S. 1 und 2 StVG an die zur Ahndung von Verkehrsverstößen zuständigen Stellen auf deren Verlangen übermittelt und von diesen gespeichert und genutzt werden. Zudem kann auch eine Übermittlung an Dritte, wie Unfallbeteiligte, geboten sein.

Als Rechtsgrundlage kommt auch die Verarbeitung auf Grundlage eines bereits geschlossenen oder sich anbahnenden Vertrages nach Art. 6 Abs. 1 S. 1 lit. b DSGVO in Betracht. In aller Regel bestehen keine vertraglichen Verhältnisse zwischen Eigentümer, Halter, Fahrer, Mitfahrer und dem Hersteller, sodass eine Heranziehung dieses Erlaubnistatbestandes häufig ausscheidet. Relevant wird die Rechtsgrundlage jedoch im Fall des oben erwähnten Telematik-Tarifs mit einer Versicherung. Hier ist die Datenverarbeitung zur Erfüllung des mit der Versicherung geschlossenen Vertrages notwendig.

Insbesondere für Hersteller interessant kann die Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 S. 1 lit. f DSGVO sein. Hier findet eine Interessensabwägung der berechtigten wirtschaftlichen, rechtlichen oder ideellen Interessen des Verantwortlichen mit den Grundrechten und Grundfreiheiten des Betroffenen statt. Diese Abwägung dürfte in Hinblick auf eine korrekte und sichere Funktionsweise des Fahrzeugs bei autonomer Steuerung oder einer anonymisierten bzw. pseudonymisierten Datenauswertung zur Verbesserung und Weiterentwicklung des autonomen Systems wohl klar zugunsten des Herstellers ausfallen und derartige Verarbeitungen als rechtmäßig statuieren, kann jedoch in zahlreichen Fällen auch anders ausfallen. So dürfte eine Verarbeitung, die durch Auswertung der Positionsdaten des Fahrzeugs Auskunft über den Gesundheitszustand des Fahrers ermöglicht (beispielsweise durch Erkenntnis häufiger Arztbesuche nach Auswertung der Positionsdaten) kaum zulässig sein.

Schließlich kommt zur Legitimierung des Verarbeitungsvorganges eine Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO infrage. Diese Einwilligung muss freiwillig, informiert, zweckbezogen und bezogen auf eine bestimmte Verarbeitung sowie unmissverständlich abgegeben werden und jederzeit widerrufbar bleiben. Ein Problem ergibt sich insbesondere bei letztgenanntem Punkt. In der Praxis ist ein Widerruf einer Einwilligung ohne Nachteile für die betroffene Person nur schwer möglich, da ein Widerruf der Einwilligung streng genommen wohl zur Folge hätte, dass das autonom fahrende Auto schlicht während der Fahrt stehenbleiben würde. Denkbar ist eine Einwilligung aus diesem Grund vielmehr nur im Bereich der Komfortfunktionen. Bei der Auswertung von Umgebungsdaten ist eine Einwilligung nicht praktikabel, da es schier unmöglich ist, die Einwilligung aller Verkehrsteilnehmer einzuholen. Hier müssen Daten also – sofern die Erhebung nicht unter einem anderen der oben genannten Zulässigkeitspunkte erlaubt ist – unverzüglich wieder gelöscht oder anonym verarbeitet werden.

Sicherheit

Schließlich hat der Verantwortliche sicherzustellen, dass die Daten entsprechend geschützt werden. So fordert Art. 24 DSGVO eine Bewertung der Schwere und der Eintrittswahrscheinlichkeit der Risiken der Verarbeitung vor ihrem Beginn durch den Verantwortlichen. Art. 32 DSGVO ergänzt diese Regelung, indem der Verantwortliche zur Implementierung geeigneter technischer und organisatorischer Maßnahmen, die ein dem Risiko angemessenes Schutzniveau der Daten gewährleisten, verpflichtet wird. Für die Entwicklung sicherer Systeme für das automatisierte Fahren müssen IT-Sicherheitsrisiken schon während der Entwicklung methodisch identifiziert, bewertet und behandelt werden. Insbesondere der Zugriff von unbefugten Dritten auf das Fahrzeug muss durch entsprechende Sicherheitskonzepte verhindert werden. Es bedarf einer Entwicklung passender Zertifizierungsverfahren für die Datensicherheit im Bereich des autonomen Fahrens, um einen einheitlichen Sicherheitsstandard zu gewährleisten.

Haftung

Aufgrund des teilweise nicht oder nur schwer vorhersehbaren Verhaltens durch neurales Lernen entstehen gewisse Risiken, weswegen ein weiterer zentraler Punkt der im Rahmen des Einsatzes von KI im Mobilitätssektor zu diskutieren ist, die Frage der Haftung darstellt. Im Folgenden wird die Haftungsfrage am Beispiel einer Verursachung eines Unfalls bei Einsatz eines autonom fahrenden Autos thematisiert.

Die Haftungsfrage hat der Gesetzgeber 2017 durch eine Änderung des StVG zu regeln versucht. Es wurde zwar das System der konkurrierenden Fahrer-, Halter- und Herstellerhaftung nach §§ 18, 7 StVG bzw. Produkthaftungsgesetz (ProdHaftG) beibehalten, die Gewichtung hat sich jedoch signifikant verschoben. Zu berücksichtigen ist auch, dass das neue System, welches insbesondere in den neuen §§ 1a und 1b StVG Niederschlag gefunden hat, bisher nur für das automatisierte bzw. hochautomatisierte Fahren gilt, während das vollständige automatisierte Fahren weiterhin nicht zugelassen ist und folglich keine Regelungen hierfür existieren.

Während die Halterhaftung bis auf eine Veränderung in der Höchstsumme unverändert bleibt, bestehen für den Hersteller gewisse Pflichten, die als Definition „getarnt" in § 1 a Abs. 2 S. 1 StVG die wesentlichen Anforderungen an ein autonomes System statuieren, damit es nicht als fehlerhaft i.S.d. Produkthaftungsrechts gilt. So muss das autonome System zur Fahrzeugsteuerung fähig sein, während der automatisierten Fahrzeugsteuerung den geltenden Verkehrsvorschriften gerecht werden können, durch den Fahrzeugführer manuell übersteuerbar oder deaktivierbar sein, die Erforderlichkeit einer eigenhändigen Fahrzeugsteuerung durch den Fahrer detektieren können, zur Anzeige des Erfordernisses einer eigenhändigen Fahrzeugsteuerung fähig sein und auf eine der Systembeschreibung zuwiderlaufenden Verwendung hinweisen können. Mangelt es an einer dieser Voraussetzungen, so besteht grundsätzlich ein Produkthaftungsanspruch. Zu berücksichtigen ist an dieser Stelle jedoch, dass der entsprechende Fehler bereits bei Inverkehrbringung (regelmäßig also bei der Zulassung) vorgelegen haben muss. Dies wird in der Regel aufgrund der damit verbundenen Beweisschwierigkeiten dazu führen, dass der Geschädigte diesen Weg nur schwer gehen kann.

Die Haftung des Fahrers mit den in §1b Abs. 2 StVG konkretisierten Verhaltensanforderungen orientiert sich an den Pflichten des Herstellers. So darf der Fahrer sich zwar vom Verkehr abwenden, muss jedoch jederzeit wahrnehmungsbereit bleiben. Er muss Warnungen des Systems sofort Folge leisten und bei Bedarf die Führung des Fahrzeuges übernehmen. Für den Fall, dass eine frühzeitige Warnung des autonomen Systems aufgrund eines Fehlers vorlag, der Fahrer jedoch trotz der Aufforderung eines Eingriffes nicht reagiert hat und ein Unfall verursacht wurde, so haftet aufgrund der fehlenden Fehlerkausalität allein der Fahrer.

Fazit

Das Themenfeld der künstlichen Intelligenz bedarf dringend regulatorischer Klarstellungen durch den Gesetzgeber. Denn KI existiert bereits und profitiert nicht von den derzeitigen ethischen, politischen und rechtlichen Debatten, die in abstrakten Sphären schweben anstatt konkrete Handlungsanweisungen für die Konzeption von KI-Systemen zu liefern. Untätigkeit vonseiten der Politik gefährdet durch eine unklare Rechtslage den technologischen Fortschritt. Die Bundesregierung hat in ihrer KI-Strategie zwar das Potenzial künstlicher Intelligenz erkannt und erste Schritte in die richtige Richtung unternommen, bis zu einer wettbewerbsfähigen „AI made in Germany" ist es jedoch noch ein weiter Weg. Die DSGVO hält entsprechende Vehikel zur Aufstellung datenschutzrechtlicher KI-Grundregeln bereit, die durch die entsprechenden Organe auch genutzt werden sollten. So bieten sich insbesondere die Aufstellung von Verhaltensregeln gem. Art. 40 DSGVO oder Stellungnahmen bzw. Leitlinien des Datenschutzausschusses nach Art. 70 DSGVO an. Angesichts des bisher noch lückenhaften regulatorischen Rahmens bleibt es spannend, wie der Einsatz von künstlicher Intelligenz im Mobilitätssektor in der Zukunft geregelt wird.

Thilo Weichert

Tesla – Überwachungsmobil und Datenschleuder

Am 17.09.2020 berichtete das ARD-Magazin Kontraste über Datenschutzverstöße durch Tesla, den US-amerikanischen Hersteller von Autos mit Elektroantrieb, die autonom oder zumindest halbautomatisiert auf Straßen unterwegs sein können. Am Tag darauf wurde Tesla in Bielefeld der BigBrotherAward, der Negativpreis für „Datenkraken", in der Kategorie Mobilität verliehen. Damit steht ein Unternehmen in der Kritik, das ansonsten positiv im Fokus der Öffentlichkeit steht: wegen seiner Innovationskraft, der angeblichen Klimaneutralität seiner Produkte oder der Schaffung von Arbeitsplätzen im brandenburgischen Grünheide.

I. Digitalisierte Individualmobilität

In der Automobilwirtschaft erfolgt derzeit ein grundlegender Wandel. Das Kraftfahrzeug (Kfz) war bisher ein weitgehend analog funktionierendes Verkehrsmittel mit Verbrennungsmotor. Die Klimakrise zwingt dazu, alternative Energieformen zu nutzen; am weitesten fortgeschritten ist der Elektromotor. Parallel dazu findet eine **Digitalisierung** in und um das Auto statt, mit der die Sicherheit und der Komfort bei der Nutzung erhöht werden sollen. Die Sicherheit wird u.a. verbessert durch Assistenzsysteme, mit denen das Spur- und Bremsverhalten beeinflusst werden, durch automatisch auslösende Airbags oder eCall-Systeme, mit denen die Folgen von Unfällen gemildert werden sollen.[1] Beim Tesla Modell 3 gibt es u.a. einen Spurhalteassistenten, einen Tempomat mit Abstandregelung, automatische Notbremsung, Warnung vor vorderen Kollisionen und Seitenaufprall.[2] Der Komfortgewinn erfolgt über Navigationssysteme, die den Weg zum Ziel leiten, über individuelle Standardeinstellungen für den Fahrer bis hin zu elektronischen Unterhaltungs- und Serviceangeboten. Einparken wird zum Kinderspiel.[3] Solche Angebote erleichtern das Führen von Kfz mit der – noch vagen – Aussicht, dass künftig die Autos ohne nötige Intervention des Fahrers autonom ans Ziel kommen. Über „Homelinks" können selbst Aktivitäten zu Hause beim Halter, z.B. das Öffnen des Garagentors, ausgelöst werden.[4]

Die deutsche Automobilwirtschaft hat diese Entwicklungen zunächst verschlafen und versucht nun ihren Innovationsrückstand aufzuholen. Unternehmen aus den USA und China geben mit mehr Patenten und attraktiven Produkten auf dem neuen Markt den Ton an. Informationstechnik-(IT-)Unternehmen, die mit Internetgeschäften ihr Kapital angehäuft haben, drängen auch auf diesen Markt. Die informationstechnische Ausstattung des Kfz gewinnt für die Kaufentscheidung eine zunehmende Bedeutung.

Datenschutz spielt bisher in der öffentlichen Diskussion über die eMobilität eine untergeordnete Rolle. Die analoge Mobilität war weitgehend anonym. Die Digitalisierung lässt nun personenbezogene Daten anfallen; die Verkehrsteilnehmer werden erfasst, gespeichert und ausgewertet. Diese mobilitätsbedingt anfallenden Daten haben ökonomisch einen Wert. Ihre Bestimmung ist es – wie schon bisher die der Internetnutzungsdaten – das „Öl des 21. Jahrhunderts" zu werden. Wer die Daten hat, hat die Kontrolle über die mobilen Menschen und die Grundlage für völlig neue Geschäftsmodelle.

II. Smartmobile auf vier Rädern

Im US-Unternehmen Tesla bündeln sich diese Entwicklungen wie in einem Brennglas: Es tritt mit seinen hochdigitalisierten Elektroautos gegen die noch stark konventionell ausgerichtete deutsche Autoindustrie an und erfasst seine Kunden sowie die Verkehrsteilnehmer generell. Die Verleihung des BigBrotherAwards (BBA) an das Unternehmen weist auf eine neue Gefahr für den Datenschutz hin die es sich zu analysieren lohnt. Anknüpfungsobjekt der BBA-Verleihung ist das Tesla Modell 3, das auch in Kürze im brandenburgischen Grünheide produziert werden soll.

Zitat aus der Laudatio[5]: Eine zentrale Funktion der Tesla-Autos ist die Video- und Ultraschallüberwachung sowohl im Fahr- als auch im Parkmodus: „Acht Kameras gewähren eine 360-Grad-Rundumüberwachung der Fahrzeugumgebung in bis zu 250 Meter Entfernung. Ergänzt werden sie durch zwölf aktualisierte Ultraschallsensoren."

Diese Sensoren dienen der Fahrerassistenz und der „Autopilot"-Funktion, also dem halbautonomen Fahren. Sie dienen auch als Ergänzung der Dashcams, um bei Unfällen im Nachhinein Informationen auszulesen. Unabhängig von einem Unfall lassen sich per Knopfdruck jeweils die letzten 10 Minuten abspeichern. Und über die USB-Schnittstelle können die einlaufenden Daten dauernd ausgelesen und ausgewertet werden.

Schaltet man die Kameras in den seit 2019 verfügbaren „Wächtermodus", den „Sentry-Mode", erfassen sie zudem dauernd die Umgebung. Bemerkt eine Kamera eine auffällige Bewegung, leuchtet auf dem Bildschirm ein roter Punkt auf und es erfolgt eine Aufzeichnung. Dafür genügt es, dass eine Person nahe am Auto vorbeigeht oder ein anderes Auto nahe vorbeifährt. Auf Youtube können Hunderte solcher Clips besichtigt werden. Bei einer Erschütterung oder einem Eindringen ins Fahrzeug wird auf einem Smartphone Alarm geschlagen und auf Wunsch dreht vor Ort die Stereoanlage automatisch voll auf.

Was mit der Technik möglich ist, zeigte der Sicherheitsforscher Truman Kain, der mit wenig Aufwand einen „Surveillance Detection Scout" bastelte, einen Minicomputer, den er mit der USB-Schnittstelle von Tesla-Fahrzeugen verbunden hat. Damit konnte er sämtliche Kameras im laufenden Betrieb auswerten, Kfz-Kennzeichen erfassen und sogar Gesichtserkennung durchführen. Registriert der Scout z.B. wiederholt

das gleiche Kennzeichen, so sendet er automatisch eine Benachrichtigung an das Handy des Halters sowie auf den Autobildschirm: „Ein Auto verfolgt dich".

Eine weitere Kamera befindet sich in den Tesla-Modellen 3 und Y im Innenraum, oberhalb des zentralen Rückspiegels. Sie ist auf die Fahrzeuginsassen gerichtet. Der Tesla-Chef Elon Musk rechtfertigte in einem Video diese Kamera damit, dass seine Autos für Fahrtenvermittlungen oder als selbstfahrende Taxis genutzt werden sollen. Über die Innenkamera könnten Dritte bei Beschädigungen und Verschmutzungen zur Verantwortung gezogen werden.

Musk ist damit längst nicht am Ende seiner Überwachungsphantasien. Per Twitter teilte er mit, untermalt von Musik, dass seine Firma an einem Feature arbeitet, das Tesla-Modelle mit Passanten sprechen lässt. In einem Video spricht dann ein „Model 3" einen Fußgänger an: „Steh nicht nur herum und starr mich an – steig ein." Musk erklärt dazu: „Teslas werden bald mit Menschen sprechen, wenn ihr das wollt. Das ist real." Nicht mehr lange, und diese geparkten Autos mischen sich ungebeten in Gespräche ein, wenn wir uns bei einem Spaziergang in Ruhe unterhalten wollen.

Was mit den durch die Autos erhobenen Daten passiert, müsste aus den Allgemeinen Geschäftsbedingungen (AGB) von Tesla abzulesen sein, mit denen eigentlich auch den datenschutzrechtlichen Informationsanforderungen gemäß Art. 12 ff. DSGVO genügt werden müsste. Dort heißt es:

Wir erfassen möglicherweise auf unterschiedlichen Wegen Informationen von Ihnen oder über Sie (beispielsweise Name, Adresse, Telefonnummer, E-Mail, Zahlungsinformationen, Führerschein- oder andere behördliche Ausweisinformationen) oder Ihre Geräte.[6]

Hinter den „Geräten" verbergen sich PC, Smartphone, aber insbesondere „Ihr Tesla-Fahrzeug". Über dieses werden „Telematikprotokolldaten", „Fernanalysedaten", „Fahrsicherheits-Analysedate", „Wartungshistorie", „Ladevorgangsinformationen", „Autopilot-Informationen", „Erweiterte Funktionen", wozu „Navigationsdaten" sowie „kurze Videoaufnahmen von den Außenkameras des Fahrzeugs" gehören, erfasst.[7]

Eine Analyse des vom Tesla aus erfolgenden Datentransfers ergab, dass eine teilweise stundenlange Datenübertragung auf Server an der US-amerikanischen Westküste erfolgt. Dabei wird eine WLAN-Verbindung genutzt. Welchen Inhalt die per WLAN übertragenen Daten haben, blieb unklar, da die Datenpakete verschlüsselt übermittelt werden.[8]

Dazu erklären die AGB: Mit der Nutzung unserer Produkte oder Dienstleistungen ... erklären Sie sich mit der Übermittlung von Informationen von Ihnen, über Sie oder über Ihre Nutzung ... in Länder außerhalb Ihres Wohnsitzlandes, einschließlich der USA, einverstanden.[9]

Angeblich werden bei Tesla in den USA die Daten umgehend weitgehend anonymisiert, wobei dies angesichts der Datendichte und der Einzelzuordnungsmöglichkeiten zu einem Kfz allenfalls eine Pseudonymisierung im Sinne des europäischen Rechts sein kann. Das Unternehmen speichert in jedem Fall die Fahrzeug-Identifizierungsnummer (FIN) mit: Wir erfassen Informationen darüber hinaus in einer Form, die für sich genommen keine direkte Verbindung mit einer bestimmten Person zulässt. Wir können nicht persönlich identifizierbare Daten für jeden Zweck sammeln, verwenden, übertragen und offenlegen. Wenn wir nicht persönlich identifizierbare Daten mit Ihren personenbezogenen Daten kombinieren, werden die kombinierten Informationen als personenbezogene Informationen behandelt, solange sie kombiniert bleiben.[10]

Zur Aufbewahrungsdauer der personenbeziehbaren Daten gibt Tesla keine verbindlichen Auskünfte. Vielmehr erklärt es, die Daten so lange aufzubewahren, „wie es erforderlich ist", „es sei denn eine längere Aufbewahrungsfrist ist rechtlich zulässig oder vorgeschrieben".[11] Für den Fall des Kfz-Weiterverkaufs ermöglicht die Technik eine Datenlöschung, aber nur „im Auto"; bei Tesla bleiben die Daten gespeichert.[12]

III. Datenübermittlungen und -nutzungen

Hinsichtlich der Datenübermittlung an Dritte scheint Tesla sehr restriktiv zu sein. Für die wertvollen Daten möchte sich Tesla das ausschließliche Nutzungsrecht bewahren und gibt Daten nur an „Dienstleister und Geschäftspartner" weiter sowie an „gesetzlich vorgeschriebene Dritte".[13] Über die Einbindung von externen Applikationen in die Autosoftware ist wenig bekannt. Beim Navigationssystem erfolgt bisher (noch) eine Nutzung von Google Maps.[14] Tesla will sich aber von diesem Dienst freimachen, offenbar, um zu verhindern, dass die Lokalisierungsdaten weiter von dem Drittunternehmen – das zugleich Konkurrent ist – genutzt werden können. Eine Eigenvermarktung der Daten schließt Tesla nicht aus. Das Unternehmen sucht vielmehr Geschäftsmodelle, über welche mit den erfassten Daten zusätzliches Geld verdient werden kann.

Sollen mit den Daten von Tesla Unfälle oder Rechtsverstöße aufgeklärt werden, so gibt das Unternehmen diese auf Anforderung an die Polizei weiter: So war in einem Fall durch die Aufnahmen der Tesla-Seitenkameras erkennbar gewesen, dass ein „Unfallverursacher log und schon vor dem Unfall rücksichtslos und mit erhöhter Geschwindigkeit auf der rechten Spur überholt hatte".[15] Gemäß einem anderen Pressebericht war im September 2018 in Berlin ein Tesla in einer 80er-Zone mit 197 km/h geblitzt worden. Per Gerichtsbeschluss sei darauf Tesla aufgefordert worden, die gespeicherten Daten herauszugeben: „Das Ergebnis: Der Tesla hatte im Sekundentakt Position und Tempo an die Zentrale gefunkt. Die Polizei konnte so die gesamte Tour rekonstruieren und herausfinden, dass der Fahrer auf der tempobegrenzten Stadtautobahn bis zu 209 km/h schnell unterwegs war."[16]

IV. Verbraucherrecht

In den AGB behält sich Tesla die eigenmächtige Änderung der Geschäftsbedingungen vor: Änderungen dieser Datenschutzrichtlinie werden wirksam, sobald wir die überarbeitete Datenschutzrichtlinie über die Dienstleistungen veröffentlichen. Durch die Nutzung unserer Produkte oder Dienstleistungen oder dadurch, dass Sie uns auf andere Weise Informationen nach diesen Änderungen zur Verfügung stellen, nehmen Sie die überarbeitete Datenschutzrichtlinie an.[17] Eine vorangehende Informa-

tion der Kunden wird nicht zugesichert. Tatsächlich kann festgestellt werden, dass solche Änderungen erfolgen. Tesla hält es – entgegen den Zusagen in den AGB an anderer Stelle – nicht einmal für nötig den Zeitpunkt der Veröffentlichung der aktuellen AGB-Version bekanntzugeben. Durch das Fehlen einer Datumsangabe ist es dem Nutzer nicht möglich festzustellen, seit wann die Regelung gilt. Es ist ihm auch nicht möglich diese mit evtl. zum Vertragsabschlusszeitpunkt geltenden AGB zu vergleichen. Damit verstößt Tesla gegen das sich aus § 307 Abs. 1 S. 2 BGB ableitende Transparenzgebot.[18]

Ein weiterer Verstoß gegen das Transparenzgebot besteht darin, dass die AGB nicht in ihrer Gesamtheit aufrufbar sind. Vielmehr enthalten sie in einigen relevanten Bereichen nur thematische Beschreibungen. Für den Aufruf der Erläuterungen bedarf es jeweils eines weiteren Klicks. Gemäß § 312i Abs. 1 Nr. 4 BGB ist der Verwender im elektronischen Geschäftsverkehr verpflichtet AGB jederzeit abrufbar zu halten und zu ermöglichen, dass sie in einer wiedergabefähigen Form abgespeichert werden können. Das Abrufen und vollständige Abspeichern verursacht bei den Tesla-AGB einen Aufwand, der von einem durchschnittlichen Kunden nicht verlangt werden kann.

Gemäß § 307 Abs. 1, 2 Nr. 1 BGB sind AGB unwirksam, wenn Bestimmungen „mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren" sind. Gesetzliche Regelungen in diesem Sinne sind auch solche des Datenschutzrechts. Für die Beurteilung der Wirksamkeit gilt in Umkehrung zu § 305c Abs. 2 BGB der Grundsatz der kundenfeindlichsten Auslegung.[19] Im Sinne des Verbraucherschutzes muss angenommen werden, dass ein Unternehmen alles, was es in seinen AGB erklärt, auch zu tun gedenkt.

Zudem gilt bei den AGB gemäß § 307 Abs. 1 S. 2 BGB das Verständlichkeitsgebot. Der Kunde muss ohne weitere Kenntnisse und Recherchen erkennen können, welche Rechte und Pflichten bei Vertragsschluss auf ihn zukommen.[20] Damit korrespondieren die verbraucherrechtlichen Anforderungen mit den Transparenzanforderungen, denen Tesla nicht im Ansatz genügt.

V. Anwendbarkeit des Datenschutzrechts

Bei der Lektüre der AGB von Tesla überrascht, dass dort an keiner Stelle die in der Europäischen Union (EU) anwendbare Datenschutz-Grundverordnung (DSGVO) erwähnt wird. Dies erklärt sich damit, dass Tesla offenbar vermeiden wollte, Extraregeln für die EU festzulegen. Bei den AGB dürfte es sich so um weltweit geltende, ins Deutsche übersetzte Regeln handeln, bei denen kein Unterschied gemacht wird, ob das Auto in einem Rechtsstaat unterwegs ist oder nicht. Dennoch behauptet Tesla in öffentlichen Äußerungen die Regeln der DSGVO zu beachten ohne dies näher zu begründen: Unsere Datenverarbeitungsaktivitäten obliegen der notwendigen Rechtsgrundlage im Einklang mit der DSGVO.[21] Eine nähere Betrachtung ergibt jedoch, dass dem nicht so ist.

Dies zeigt sich schon bei Teslas Ausführungen zur datenschutzrechtlichen Verantwortlichkeit. Zwar erklärt sich das Unternehmen zunächst verantwortlich für die im Auto und aus dem Auto heraus vorgenommene Datenverarbeitung: Wenn Sie im EWR, in Großbritannien oder in der Schweiz ansässig sind, ist Tesla International B.V. für die Verarbeitung Ihrer personenbezogenen Informationen verantwortlich. Offenbar unterstellt das Unternehmen, dass Tesla-Kunden so gebildet sind, dass diese wissen, dass „EWR" Europäischer Wirtschaftsraum" bedeutet und dass hierzu sämtliche Mitgliedstaaten der EU gehören. Doch bleiben die Kunden im Dunkeln, wer sich hinter der „Tesla International B.V." verbirgt. Erst eine tiefere Recherche ergibt dann möglicherweise, dass es sich hierbei um eine Tesla-Niederlassung in Amsterdam/Niederlande handelt.

Nicht nur intransparent, sondern falsch wird es, wenn bzgl. der Dashcams von Tesla behauptet wird, für deren Bilder sei ausschließlich der Tesla-Kunde verantwortlich. Er ist ja über eine USB-Schnittstelle in der Lage diese Bilder auszuleiten, abzuspeichern und auszuwerten. Die Kundenverantwortlichkeit besteht danach, es sei denn, das lokale Gesetz verbietet generell den Verkauf von Dash-Cams oder überträgt auf andere Weise die Verantwortung auf den Verkäufer.[22] Tesla setzt damit Rechtskenntnisse bei Kunden voraus, die dieser regelmäßig nicht hat.

Nach der neueren Rechtsprechung des EuGH kann zudem Tesla nicht leugnen, dass dem Unternehmen auch insofern regelmäßig eine „gemeinsame Verantwortlichkeit" mit dem Kfz-Halter zukommt.[23] Und diese gemeinsame Verantwortlichkeit geht über den Dashcam- bzw. Wächtermodus-Einsatz hinaus und betrifft sämtliche Daten, die nicht über den Halter selbst, sondern in identifizierbarer Form über Dritte verarbeitet werden, etwa über andere Fahrer und Verkehrsteilnehmer. Negiert Tesla damit überhaupt eine „gemeinsame Verantwortlichkeit", so ignoriert das Unternehmen konsequenterweise auch die rechtlichen Anforderungen des Art. 26 DSGVO, wonach mit dem mitverantwortlichen Halter eine Vereinbarung abgeschlossen werden muss, die das Nähere zur gemeinsamen Verantwortung regelt.

VI. Rechtmäßigkeit

Allzu leicht macht es sich Tesla auch mit der Benennung der anzuwendenden Rechtsgrundlagen: Wir können uns für die Erhebung, Nutzung und anderweitige Verarbeitung Ihrer Informationen auf verschiedene Rechtsgrundlagen berufen, einschließlich: Sie haben Ihre Einwilligung gegeben; die Informationen sind für die Erfüllung des Vertrags mit Ihnen erforderlich; die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich; die Verarbeitung ist erforderlich, um Ihre lebenswichtigen Interessen oder die einer anderen natürlichen Person zu schützen; oder für die Wahrung eines berechtigten Interesses, das gegen Ihre Interessen, Grundrechte- und Grundfreiheiten abgewogen wird. Diese berechtigten Interessen können Teslas Interesse an der Verbesserung eigener Produkte oder Dienstleistungen, der Erhöhung von Sicherheit, dem Schutz von Tesla oder Teslas Geschäftspartnern gegen unrechtmäßiges Verhalten und die Beantwortung von Kundenanfragen oder Beschwerden beinhalten. Wir werden Sie gegebenenfalls informieren, ob und aus welchem Grund wir gewisse Informationen von Ihnen benötigen, beispielsweise, ob wir diese Informationen



Bild: Frans Valenta

für die Erfüllung einer rechtlichen oder vertraglichen Verpflichtung benötigen und was die Folgen sind, wenn diese Informationen nicht zur Verfügung gestellt werden.

Die Allerweltsaussage in den AGB genügt nicht den Anforderungen der Art. 13 und 14 Abs. 1 lit. c DSGVO, wonach der Betroffene über die jeweilige Rechtsgrundlage zu informieren ist. Die Wiedergabe aller möglichen Rechtsgrundlagen, wie sie in Art. 6 Abs. 1 UAbs. 1 DSGVO aufgeführt sind, genügt der Transparenzpflicht nicht, die dem Betroffenen im Einzelfall die Überprüfung ermöglichen soll, ob sich die jeweilige Verarbeitung im Rahmen einer Einwilligung, der Erforderlichkeit des Vertrags oder einer angemessenen Interessenabwägung bewegt.

Unzulässig ist bei Tesla-Fahrzeugen in jedem Fall die hierdurch erfolgende Dauerüberwachung der Fahrzeugumgebung im öffentlichen Raum. Wenn Menschen gefilmt und deren Daten aufgezeichnet werden, die nur an einem Auto vorbei gehen, ohne dass sie sich konkret verdächtig machen, ist dies klassische illegale Vorratsdatenspeicherung. Im öffentlichen Raum rund um ein Tesla-Fahrzeug wird gefilmt und möglicherweise identifiziert, je nachdem, welche Technik im Auto aktiv ist.[24] Die Betroffenen wissen nicht, was davon das Auto gerade tut.[25] Es erfolgt keine Information der Betroffenen (Art. 13, 14 DSGVO). Die Erforderlichkeit dieser Vollerfassung für konkrete Zwecke ist nicht gegeben. Es sind keine Schutzmaßnahmen erkennbar, mit denen die Rechte der Betroffenen hinreichend gewahrt würden.

Diese Aussagen gelten in besonderem Maße für den sog. „Wächtermodus“. Dieser zielt vorrangig ab auf eine Datenerhebung über Dritte, die völlig unbeteiligte Verkehrsteilnehmer sind, ohne dass präzise Zwecke festgelegt werden und hinreichende Vorkehrungen für die Betroffenen bestünden.

Eindeutig unzulässig sind auch die Datenübermittlungen in die USA. Für diese beruft sich das Unternehmen auf die Anwendung des Privacy Shields.[26] Mit Urteil vom 16.07.2020 hat der EuGH festgestellt, dass ab sofort das Privacy Shield keine gültige Rechtsgrundlage für eine Datenübermittlung in die USA ist.[27] Soweit sich Tesla auf Standarddatenschutzklauseln beruft, wird im gleichen Urteil festgestellt, dass diese allein eine Datenübermittlung z.B. in die USA nicht legitimieren können. Vielmehr ist es nötig, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung eines angemessenen Schutzniveaus zu gewährleisten. Dies ist insbesondere bei Übermittlungen in die USA nötig, da dort Regelungen gelten, die eine Massenüberwachung zulassen und es dort weder eine unabhängige Datenschutzaufsicht noch einen hinreichenden Rechtsschutz gibt.[28] Derart zwingend geforderte Schutzmaßnahmen hat Tesla nicht vorgesehen.

Tesla beruft sich zudem auf die Einwilligung der Betroffenen für die Datenübermittlung in Drittländer ohne angemessenes Datenschutzniveau. Eine solche Legitimation wäre nach Art. 49 Abs. 1 lit. a DSGVO aber nur im Ausnahme- und Einzelfall zulässig, wenn zugleich auf die besonderen Übermittlungsrisiken explizit hingewiesen wird. Davon kann bei Tesla aber keine Rede sein.

VII. Ergebnis

Aus den obigen Ausführungen ergibt sich, dass die Datenverarbeitung durch Tesla in vieler Hinsicht gegen die Vorgaben des europäischen Datenschutzes und des Verbraucherschutzes verstößt:

- Tesla benennt für die jeweilige Datenverarbeitung keine präzisen Zwecke und verstößt damit gegen Art. 5 Abs. 1 lit. b DSGVO.
- Tesla gibt nicht an, auf welcher Rechtsgrundlage gemäß Art. 6 Abs. 1 UAbs. 1 DSGVO die jeweils von ihr vorgenommene Datenverarbeitung basiert.
- Tesla genügt nicht den Anforderungen an die Datenminimierung und die Erforderlichkeit bei der Datenverarbeitung gemäß Art. 5 Abs. 1 lit. c, 6 Abs. 1, 25, 32 DSGVO.
- Tesla ist insbesondere mitverantwortlich für die nicht erforderliche umfassende und uneingeschränkte Videoüberwachung und die darauf folgende Verarbeitung sowohl im Fahr- als auch im Parkmodus, wenn der Wächtermodus eingeschaltet ist.

- Tesla benennt nicht die von dem Unternehmen vorgenommene Datenverarbeitung und informiert nicht über die Betroffenenrechte in einer hinreichend „präzisen, transparenten, verständlichen und leicht zugänglichen Form in einer klaren und einfachen Sprache" und verstößt damit gegen Art. 12 Abs. 1 DSGVO.
- Tesla genügt nicht seiner Informationspflicht nach den Art. 13, 14 DSGVO, indem es unterlässt über folgende Angaben präzise Informationen zu geben: Zwecke, Rechtsgrundlage, berechtigtes Interesse, fehlende Angemessenheit im Empfängerland, Speicherdauer.
- Tesla übermittelt unter Verstoß gegen die Art. 44 ff. DSGVO Daten in die USA sowie evtl. in weitere Staaten ohne angemessenes Datenschutzniveau.
- Tesla ignoriert die eigene datenschutzrechtliche Verantwortlichkeit beim „Wächtermodus" und schließt mit den Kfz-Haltern keine nach Art. 26 DSGVO geforderte Vereinbarung ab.
- Die AGB von Tesla verstoßen sowohl in formeller als auch in inhaltlicher Hinsicht gegen die Vorgaben der §§ 305 ff. BGB.

Dieses aus datenschutzrechtlicher Sicht vernichtende Urteil hat nun aber leider nicht zur Folge, dass den Tesla-Fahrzeugen die Typenzulassung gemäß der Straßenverkehrszulassungsordnung entzogen wird. Datenschutz spielt dabei (bisher noch) keine Rolle, obwohl mit der Kfz-Digitalisierung die Anforderungen an die Sicherheit im Straßenverkehr und an den Datenschutz immer mehr zusammenfließen.

Gefordert sind angesichts der Rechtsverstöße zunächst die Datenschutzbehörden, die aber anlässlich der aktuellen Berichterstattung schon durchblicken ließen, dass sie sich derzeit mit der Durchsetzung des Datenschutzes gegenüber einem Player wie Tesla überfordert fühlen.[29] Verbraucherschutzorganisationen könnten über eine Verbandsklage nach dem Unterlassungsklagegesetz (Art. 80 Abs. 2 DSGVO) umgehend gegen Datenverarbeitung von Tesla und die von dem Unternehmen verwendeten AGB vorgehen. Gefordert ist auch die Politik, der nicht nur Elektromobilität und Arbeitsplätze, sondern auch der Datenschutz ein Anliegen sein sollte. Letztlich sollte es sich jeder Verbraucher genau überlegen, ob er in einem Überwachungsgefährt und einer Datenschleuder unterwegs sein möchte, die sein gesamtes Mobilitätsverhalten und das seines Umfelds erfasst und teilweise in die USA übermittelt, wo dann bei Bedarf US-Geheimdienste auf diese Daten zugreifen können.

1 Grundlegend Bönninger in 52. Deutscher Verkehrsgerichtstag 2014, S. 230 ff.; aktuell Becker, Kopf an Kopf, SZ 20./21.06.2020, 45.

2 Schurter, Daniel, Warum Teslas „Wächtermodus" auch jeden Fußgänger betrifft, 24.09.2019, https://www.watson.ch/digital/tesla/337037325-videoueberwachung-durch-tesla-fahrzeuge-was-man-wissen-sollte.

3 Tesla, Model 3 Benutzerhandbuch, Software-Version 2020.20 Europe, S. 75 f., 117 ff.

4 Tesla Benutzerhandbuch (En. 3), S. 162 ff.

5 https://bigbrotherawards.de/2020/mobilitaet-tesla.

6 https://www.tesla.com/de_DE/about/legal#collect.

7 https://www.tesla.com/de_DE/about/legal#collect.

8 Humbs/Weller, Gläserner Autofahrer – Verstößt Tesla gegen Datenschutzregeln? https://www.tagesschau.de/investigativ/kontraste/tesla-datenschutz-101.html; Kontraste, ARD 17.09.2020, Autoren: Humbs, Chris/Weller, Marcus, Fernseh-Beitrag zu Tesla; Rudin/Gysin, (Hrsg. Datenschutzbeauftragter des Kantons Basel-Stadt), Vorabkontrolle: Schlussbericht Alarmpikettfahrzeuge der Kantonspolizei, 26.04.2019, https://www.dsb.bs.ch/dam/jcr:be059e63-d032-4817-9381-5227de60c7f3/Schlussbericht_Vorabkontrolle_Intelligente_Fahrzeuge_final_20190426_(Web).pdf, S. 13.

9 https://www.tesla.com/de_DE/about/legal#privacy-shield.

10 https://www.tesla.com/de_DE/about/legal#collect.

11 https://www.tesla.com/de_DE/about/legal#collect.

12 Tesla Benutzerhandbuch (En. 3), S. 138.

13 Tesla Benutzerhandbuch (En. 3), S. 138.

14 Evannex, Elon Musk Says Tesla Will Build Its Own Maps From GPS & Fleet Data, 18.04.2020, https://insideevs.com/news/410425/tesla-maps-driving-data-elon-musk/; unklar insofern Tesla Benutzerhandbuch (En. 3), S. 146.

15 Schurter (En. 2).

16 Schmidt-Kasparek, Darf Polizei Fahrzeugdaten nutzen? 25.09.2019, https://www.firmenauto.de/unfall-mit-firmenwagen-darf-polizei-fahrzeugdaten-nutzen-10904161.html.

17 https://www.tesla.com/de_DE/about/legal#choice-transparency.

18 Mäsch in Staudinger BGB, §§ 305-310, UKlaG, 2019, § 307 Rn. 180; Grüneberg in Palandt, Bürgerliches Gesetzbuch, 78. Aufl. 2019, § 305 Rn. 20 f.

19 BGH NJW 2008, 360, Rn. 28.

20 Grüneberg in Palandt, Bürgerliches Gesetzbuch, 78. Aufl. 2019, Rn. 25.

21 E-Mail von Tesla vom 18.09.2020.

22 E-Mail von Tesla vom 18.09.2020.

23 EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = NZA 2018, 919 = ZD 2018, 357 = NVwZ 2018, 1386 = EuZW 2018, 534 = MMR 2018, 591 = BB 2018, 1480 = DuD 2018, 518; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; EuGH 29.07.2019 – C-40/17 (Fashion ID), NJW 2019, 2755 = NZA 2019, 1125 = MMR 2019, 579 = BB 2019, 1995 = K&R 2019, 562 = DuD 2019, 723.

24 DSK, Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), 28.01.2019; Lennart NZV 2020, 71 ff.; Greger DAR 2018, 507; Buchner/Petri in Kühling/Buchner, Art. 6 Rn. 172d; zur Rechtslage vor der Geltung der DSGVO BGH 15.05.2018 – VI ZR 233/17, NJW 2018, 2883 = NZV 2018, 367 = MDR 2018, 990 = VersR 2018, 1076 = MMR 2018, 602 = DAR 2018, 498 = DuD 2018, 708; Weichert SVR 2014, 246.

25 https://futurezone.at/produkte/warum-der-tesla-ueberwachungsmodus-in-oesterreich-nicht-legal-ist/400522801.

26 https://www.tesla.com/de_DE/about/legal#choice-transparency; https://www.tesla.com/de_DE/about/legal#privacy-shield

27 EuGH 16.07.2020 – C-311/18, Rn. 201, NJW 2020, 2613 = WM 2020, 1495 = DuD 2020, 685.

28 EuGH 16.07.2020 – C-311/18, Rn. 121, 133, 150 ff, 179, 182, 196, 201, Golland NJW 2020, 2593 ff.; Voigt CR 2020, 513 ff.

29 Kontraste (En. 8).

DANA-Interview (HA) mit Joachim Schwarz (JS) und Silke Weitkamp (SW) von der cambio Mobilitätsservice GmbH & Co KG

Carsharing als Firewall zu den PKW-Herstellern?

HA: Herr Schwarz, Sie sind der Geschäftsführer für den Bereich Technik und Finanzen und Frau Weitkamp, Sie sind die Datenschutzkoordinatorin der cambio Mobilitätsservice GmbH & Co. KG, der Muttergesellschaft einer großen Gruppe von Dienstleistungsunternehmen für das stationsbasierte CarSharing. Die auf Ihrer Webseite veröffentlichten Datenschutzerklärungen erscheinen übersichtlich gegliedert und verständlich. Darüberhinausgehend haben wir noch einige Fragen:

Die KG bietet den cambio-Mandanten, so steht es auf der Webseite, „in einem franchiseähnlichen Angebot […] alle zentralen Dienstleistungen". Wie stellen Sie konkret die Einhaltung der Datenschutzbestimmungen sicher?

SW: Wenn wir über Datenschutz bei cambio sprechen, betrachten wir verschiedene Ebenen. Auf technischer Ebene setzen wir Datenschutz in der Software-Entwicklung für unsere eigene CarSharing-Software, bei der Auswahl von Fremd-Software und bei der Konzeptionierung von Datenübertragungswegen um. Dadurch, dass wir die cambio CarSharing-Software selber entwickeln, haben wir maximale Kontrolle darüber, wie Daten verarbeitet werden.

Auf der Ebene von organisatorischen Maßnahmen zum Datenschutz haben wir in den letzten Jahren gelernt, dass es sinnvoll ist, neben unserem externen Datenschutzbeauftragten zusätzlich eine cambio-weite Datenschutzkoordination und Ansprechpersonen für Datenschutz in jedem einzelnen cambio-Unternehmen vor Ort zu haben. So sorgen wir durch ständige Abstimmung mit allen cambio-Unternehmen und durch regelmäßige Sensibilisierung auf allen Hierarchieebenen dafür, dass Datenschutz-Maßnahmen cambio-weit umgesetzt werden. Mittlerweile ist Datenschutz ein selbstverständlicher Teil der Abstimmungen zu jedem Thema.

HA: Wie können wir uns die Rollenverteilung und Zusammenarbeit zwischen dem externen Datenschutzbeauftragten und der Datenschutzkoordination bei cambio vorstellen?

SW: Unser externer Datenschutzbeauftragter ist für uns nicht nur eine Kontrollinstanz, sondern vielmehr ein konstruktiver Ideen- und Ratgeber. Er wird von Anfang an eng mit in alle Prozesse einbezogen - insbesondere auch wenn es um die fachliche Begleitung neuer Features und Kooperationen geht. Sein starker IT-Hintergrund ist für datenschutzgerechte technische Umsetzungen für uns von enormem Vorteil. Die Datenschutzkoordination hat zusätzlich das detaillierte Wissen über unternehmensinterne Abläufe. Zusammen können so datenschutzkonforme Lösungs- und Umsetzungskonzepte erstellt werden.

HA: Es gibt ja in einigen Regionen Deutschlands eine (mehr oder weniger) enge Zusammenarbeit mit örtlichen Nahverkehrs-Unternehmen. Wie kann sich jemand den dabei nötigen Datenaustausch vorstellen?

JS: Grob skizziert gibt es dabei momentan zwei Modelle. In der einen Variante, z. B. bei der ASEAG in Aachen, erhält cambio nicht die Namen, Adressen und Kontaktdaten der Nutzerinnen und Nutzer, sondern lediglich Chipkartennummern. Die Nutzerinnen und Nutzer tauchen in unserem System dann lediglich mit einer Chipkartennummer und der Bezeichnung des ÖPNV-Unternehmens auf. Die Abrechnung und die Kommunikation läuft (auch im Falle von Unfällen und Bußgeldern) über das ÖPNV-Unternehmen und bezieht sich auf die Chipkartennummer. Das ÖPNV-Unternehmen stellt selbst die App, das Callcenter etc.

In der zweiten Variante werden Namen, Adressen und Kontaktdaten vom Kundinnen und Kunden des ÖPNV-Unternehmens direkt auf ein Formular von cambio eingetragen. Wir erhalten die Daten also von Anfang an direkt von den Kundinnen und Kunden selbst. Ob dann die Abrechnung durch cambio direkt oder durch das ÖPNV-Unternehmen erfolgt, unterscheidet sich von Stadt zu Stadt.

Zukunftsstrategien der ÖPNV-Unternehmen gehen in Richtung MAAS (mobility-as-a-service). Die Idee dabei ist, dass alle personenbezogenen Daten für die Nutzung einer Mobilitäts-Plattform nur einmal erhoben werden und dann per Klick an- oder abgewählt werden kann, welche angeschlossenen Dienste genutzt werden sollen. Die Unternehmen wollen uns so über ihre Plattform Kundinnen und Kunden vermitteln. Diese Pläne sind bisher allerdings gescheitert, da wir nicht bereit sind Daten von Kundinnen und Kunden ohne deren Zustimmung zu unseren AGBs und zu unserer Datenschutzinformation aufzunehmen. An dieser Stelle besteht momentan also ein Konflikt zwischen dem Wunsch der ÖPNV-Unternehmen nach Usability und unserer Forderung nach rechtskonformer Verarbeitung.

HA: Seit 15 Jahren bieten die cambio-Gesellschaften neben der vorab festgelegten Fahrzeit teilweise auch sogenannte Open-End-Buchungen an. Wurden oder werden für die Planung von Open-End Buchungen auch personenbezogene Daten der Nutzenden ausgewertet?

JS: Nein, überhaupt nicht. Wir lösen das technisch viel einfacher: die Open-End Buchungen sind „normale" Buchungen mit einer angenommenen Dauer und einer automatischen Verlängerung, wenn die Kundin oder der Kunde nicht zwei Stunden vor Ende der Buchung die Fahrt beendet hat. Um dann folgende Buchungen nicht stornieren zu müssen, bieten wir Open-End-Buchungen nur an Stationen an, an denen

mindestens zwei weitere Autos des gleichen Typs vorhanden sind.

Nach und nach werden Open-End-Buchungen wahrscheinlich sowieso überflüssig. In Bremen erweitert seit August 2020 das Free-Floating Angebot von cambio unter dem Namen „smumo“ (smart urban mobility) unser stationsbasiertes Angebot. Free-Floating-Fahrzeuge werden nicht gebucht. Sie stehen einfach wieder zur Verfügung, wenn sie zurückgegeben wurden.

HA: Allgemein zur Auswertung der anfallenden Daten: An Nutzungs- und Fahrverhalten haben sicher sowohl Sie als auch andere Akteure ein großes Interesse. Wie werden die Daten ausgewertet?

JS: Wir haben von Anfang an, seit 1990, den Grundsatz: „Wir geben keine Daten an Dritte weiter und haben kein Interesse an den damit verbundenen Geschäftsmodellen.“ Wir müssen allerdings selbst verschiedene Auswertungen machen, um der Nachfrage der Kunden möglichst gut nachkommen zu können. An welchen Stationen wird z. B. ein Kombi nur gebucht, weil der Fiesta nicht frei ist? Durch die Art und Weise, wie unser Buchungssystem funktioniert, kennen wir die Buchungswünsche und stellen diese Daten wöchentlich den jeweiligen Geschäftsführerinnen und Geschäftsführern zur Verfügung, um auf Basis dieser Daten planen zu können. Damit können Stationsgrößen an den Bedarf angepasst oder auch langfristige Fahrzeugbestellungen z. B. für den Sommer geplant werden. Diese Auswertungen sind nicht personenspezifisch. Wir haben 140.000 Kundinnen und Kunden und dabei ist es unwichtig, welche Person welchen Buchungswunsch hat. Uns interessiert für die Planung die Gesamtheit aller Buchungswünsche.

HA: Sie schreiben, dass mehr als die Hälfte der Fahrten beruflich veranlasst sind. Wie detailliert sind die Fahrtdaten, die an Unternehmen übermittelt werden, deren Angestellte cambio-Fahrzeuge für Dienstfahrten nutzen. Nehmen wir an, eine Mitarbeiterin oder ein Mitarbeiter hat einen Unfall. Was wird dem Arbeitgeber übermittelt?

SW: Wir müssen zwei Szenarien unterscheiden: Bei Fremdverschulden nehmen wir Kontakt mit dem Unfallgegner auf. Wenn nötig, reden wir dann mit der Fahrerin oder dem Fahrer (also in diesem Fall der/dem Angestellten des Unternehmens) oder aber wir geben, nach deren Einwilligung, die Kontaktdaten an unseren Anwalt oder unsere Anwältin weiter, wenn das für die Bearbeitung des Vorgangs nötig ist. Der Arbeitgeber erfährt von alledem nichts.

Im Falle von Eigenverschulden wenden wir uns direkt an die Fahrerin oder den Fahrer und besprechen alles Wesentliche. Sie oder er bekommt dann eine E-Mail über die zu zahlende Eigenbeteiligung, die er oder sie an den Arbeitgeber weiterleitet, da wir die zu zahlende Summe dem Arbeitgeber in Rechnung stellen. Als Ausnahme gilt hier, wenn uns die Fahrerin oder der Fahrer bittet den Arbeitgeber direkt zu informieren. In diesem Fall verschicken wir die E-Mail an die Fahrerin oder den Fahrer und nehmen den Arbeitgeber in Kopie.

JS: Der Arbeitgeber als Vertragspartner mit cambio hat zusätzlich natürlich Zugriff auf die Fahrtdaten und kann zuordnen, zu welcher Fahrt der Schaden gehört. Im Vergleich zu einem Unfall mit einem Dienstwagen bekommt der Arbeitgeber von uns allerdings kein Unfallprotokoll.

HA: Damit wären wir schon fast am Ende des Interviews. Zu guter Letzt, was erwartet uns Ihrer Einschätzung nach noch alles in Sachen IT im KFZ?

JS: Heute ist es schon so, dass die Informationsdichte zwischen Hersteller und Auto sehr groß ist. Der Hersteller bekommt beim Autokauf den Namen der Käuferin oder des Käufers und kann dann eine Vielzahl von Daten über das Fahrzeug abrufen wie etwa Spritverbrauch, Bauteileverschleiß, Fahrverhalten. All das kann in der Regel einer Person, meist der Käuferin oder dem Käufer des Pkws, zugeordnet werden.

Im Gegensatz zum Pkw im Privatbesitz kann beim CarSharing der Autohersteller die Daten keiner Person zuordnen, denn aus Herstellersicht fährt hier immer nur der Kunde „cambio“. Wir geben die Information, wer zu welchem Zeitpunkt im Auto sitzt, nicht weiter. Wir als CarSharing-Unternehmen bilden dadurch sozusagen die Firewall zwischen Kundinnen und Kunden und den Herstellern des Pkws. Das würde für autonome Autos in der Zukunft genauso funktionieren.

Datenschutz gehört für uns zu einer langfristigen und fairen Kundenbeziehung. Wir brauchen diese Partnerschaft zu unseren Kundinnen und Kunden. Das ist die Basis, auf der wir arbeiten. Wenn dieses Vertrauen verloren geht, würden wir das sehr schnell zu spüren bekommen, denn am Ende sitzen wir alle im gleichen Boot. Es ist gemeinschaftliches CarSharing und kein reines Vermietgeschäft.

HA: Frau Weitkamp, Herr Schwarz, ich danke Ihnen für das Gespräch.



Bild: cambio

Werner Hülsmann

Datenschutz bei der Nutzung von Mietwagen

Oder: Der Versuch eine vollständige Auskunft nach Art. 15 DSGVO zu erhalten

Der Sachverhalt

Ein Bekannter des Autors – nennen wir ihn Michael Müller, da sein echter Name nichts zur Sache tut – mietet des Öfteren bei einer der führenden Autovermietungsfirmen (im folgenden „EdfAVF“ genannt, da Herr Müller darum bat, den Firmennamen nicht zu nennen) einen Mietwagen. Beruflich als Datenschützer tätig dachte sich Michael Müller, dass es doch mal interessant wäre zu erfahren, wie denn EdfAVF auf eine Auskunftsanfrage reagieren würde. So schrieb Herr Müller an EdfAVF:

„Ich wäre Ihnen dankbar, wenn Sie mir eine Auskunft gem. Art. 15 DSGVO zukommen lassen könnten. Gerne auch postalisch an die bei Ihnen zu meinem Konto hinterlegte Postanschrift.

Ich wäre Ihnen dankbar, wenn Sie mir dabei konkretisierend mitteilen könnten, wann und wie die personenbezogenen Daten inkl. dazu gehöriger Metadaten, die dadurch entstehen, dass ich mich mit meinem Handy mit dem Mietfahrzeug verbinde (idR via Bluetooth), dort wieder gelöscht werden.“

Der erste Teil des Auskunftsersuchens ist sehr allgemein gehalten. Der zweite Teil wird dagegen sehr konkret. Aus Sicht des Autors ist diese Fragestellung sehr interessant. Schließlich kommt es sicher sehr häufig vor, dass MieterInnen eines Fahrzeugs ihr Smartphone mit dem „Bordcomputer“ verbinden, um die fahrzeugeigene Freisprecheinrichtung zu nutzen oder im Smartphone gespeicherte Adressdaten an das Navigationsgerät des Mietwagens zu übertragen.

Die Auskunft

Die Antwort der Mietwagenfirma zum zweiten Punkt war so überraschend wie erstaunlich:

„Bitte gestatten Sie uns folgende Information: Wenn unsere Kunden personenbezogene Daten in den Infotainment-Systemen speichern, handelt es sich nicht um eine Datenerhebung oder Speicherung durch EdfAVF. Gemäß Ziffer X,y. unserer Allgemeinen Vermietbedingungen sorgt der Mieter selbst für eine Löschung der Daten.“

Dazu müsste den MieterInnen eine entsprechende Anleitung für das Löschen dieser Daten zur Verfügung gestellt werden. Unabhängig davon stellt sich allerdings die Frage, ob diese Antwort datenschutzrechtlich haltbar ist. So gehört doch das System, in dem diese Daten bei einer Kopplung des Smartphones mit dem Infotainment-System landen, der Vermietfirma. Von daher legt die Vermietfirma zumindest die Mittel fest, mit denen diese Daten verarbeitet werden. Durch die Auswahl des Infotainment-System sind auch die Zwecke vorgegeben zu denen dieses System genutzt werden kann. Ist dann nicht auch die Autovermietfirma als Verantwortlicher im Sinne von Art. 4 Ziff. 7 DSGVO zu sehen?

Die Antwort auf die allgemeine Auskunftsanfrage war weniger überraschend. Sie war aus Sicht von Herrn Müller unvollständig. So schrieb er erneut an EdfAVF:

„Ich habe Ihre Antwort und Auskunft nach Art. 15 DSGVO erhalten. Hierfür zunächst vielen Dank.

Ich bin mir allerdings nicht sicher, ob diese vollständig ist.

So fehlen m.E. Angaben zu folgenden Punkten, deren Verarbeitung Sie in Ihrem Datenschutz-Informationsblatt selbst angeben:

- *Kommunikationsdaten (aktuell fehlen m.E.: die Kommunikationsinhalte)*
- *Vertragsdaten (aktuell fehlen m.E.: die Beschwerde bzw. Umfragedaten; Angaben zu meinem Kundenstatus, für den ich einen Aktionärsnachweis eingereicht habe; Übergabeprotokolle; Bonitätsdaten)*
  - *Standortdaten aus der App-Nutzung*
  - *Telematikdaten*

Könnten Sie mir diese Informationen noch zur Verfügung stellen?“

Auf diese Nachfrage bekam Herr Müller weitere Information von EdfAVF. Bonitätsdaten lägen keine vor, das Vorliegen der Umfrageantworten und einer Beschwerde wurde bestätigt, ebenso dass auf Grund der Beschwerde eine Rechnung korrigiert wurde, der Kundenstatus wurde beauskunftet und „alle verfügbaren Übergabeprotokolle“ wurden in einer mit Passwort geschützten Zip-Datei übersandt, welches Herrn Müller „mit separater E- Mail“ erhielt. Zu den explizit nachgefragten Standort- und Telematikdaten wurde mitgeteilt:

„Sollten wir Ihre Standortdaten und Telematikdaten erhoben haben, so haben wir diese nur für einen kurzen Zeitraum verarbeitet. Standortdaten und Telematikdaten werden schnellstmöglich gelöscht. Es sind keine Standortdaten und Telematikdaten gespeichert.“

Soweit, so gut.

Zu den angefragten Kommunikationsinhalten wurde seitens EdfAVF beschieden:

„Kommunikationsinhalte sind nicht vom Auskunftsanspruch der Datenschutz-Grundverordnung (DSGVO) umfasst. Die für uns zuständige Datenschutzaufsichtsbehörde führt dazu aus: „Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO betrifft nach dem Wortlaut von dessen Abs. 1 eine Auskunftserteilung über die personenbezogenen Daten, die vom Verantwortlichen verarbeitet werden. Das bedeutet aber nicht regelmäßig die Herausgabe von allen Dokumenten, E-Mails etc., in denen z. B. der Name der betroffenen Person und eventuelle weitere Informationen über diese Person enthalten sind. Nach Art. 15 Abs. 3 DSGVO ist nur eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“, zur Verfügung zu stellen. Es ist hier jedoch nicht die Rede von Kopien der betreffenden Akten, von sonstigen Unterlagen usw.“ (….). Überdies beeinträchtigt die Beauskunftung Rechte und Freiheiten anderer Personen (vgl. Art. 15 Abs. 4 DSGVO), insbesondere

Betriebs- und Geschäftsgeheimnisse sowie Persönlichkeitsrechte unserer Mitarbeiter, da diese im operativen Alltag teils interne Vermerke zur Gedächtnisunterstützung und reibungslosen Abwicklung bzw. Bereitstellung unserer Mobilitätsangebote machen."

Michael Müller kommentierte diese Aussage mit

„Sportliche Auffassungen, insbesondere vor dem Hintergrund des OLG Köln Urteils"[1]

Es ist zwar richtig, dass gemäß Art. 15 Abs 4 DSGVO das Recht auf Erhalt einer Kopie der Daten, „die Rechte und Freiheiten anderer Personen nicht beeinträchtigen" darf. Allerdings ist die Verweigerung einer solchen Kopie keine adäquate Lösung. Vielmehr ist es möglich betreffende Namen oder sonstige Kürzel, die auf die Beschäftigten von EdfAVF schließen lassen, zu schwärzen, um die Persönlichkeitsrechte zu schützen. Auch die Argumentation mit „Betriebs- und Geschäftsgeheimnissen" ist in Bezug auf die Kommunikationsinhalte hier nicht zielführend. So stellt das OLG Köln im genannten Urteil fest *„Die Beklagte kann sich demgegenüber auch nicht mit Erfolg darauf berufen, dass ein entsprechend weit gefasster Datenbegriff ihre Geschäftsgeheimnisse verletzen würde."* (Randnr. 316) und verurteilt die Beklagte dazu,

*„dem Kläger über die mit Schreiben vom 10.08.2018 bereits erfolgte Übersendung einer „Aufstellung Ihrer Personendaten aus der zentralen Datenverarbeitung" sowie „Aufstellung Ihrer Personendaten aus dem Lebensversicherungsvertrag Nr. 7xx57xx0.x" hinaus Auskunft zu sämtlichen weiteren diesen betreffenden personenbezogenen Daten, **insbesondere auch in Gesprächsnotizen und Telefonvermerken**, zu erteilen, welche die Beklagte gespeichert, genutzt und verarbeitet hat."* (Hervorhebung durch den Autor).

Unter Berücksichtigung des – zum Redaktionsschluss – noch nicht rechtskräftigen Urteils ist auch mit dem zweiten Schreiben der Auskunftsanspruch noch nicht erfüllt. Daher wäre dies eigentlich ein Fall für die Datenschutz-Aufsichtsbehörde. Ob Michael Müller diesen Weg beschreiten wird, war zum Redaktionsschluss noch offen.

Fazit

Nicht nur beim Thema autonomes Fahren ist die Umsetzung des Datenschutzes noch verbesserungsfähig. Auch bei einem schon lange genutzten Geschäftsmodell wie der Autovermietung ist der Datenschutz und insbesondere die Umsetzung des Auskunftsrechts ausbaufähig.

1 Urteil des Oberlandesgericht Köln, 20 U 75/18, zu finden unter: http://www.justiz.nrw.de/nrwe/olgs/koeln/j2019/20_U_75_18_Urteil_20190726.html

Heinz Alenfelder

Moderne Fahrrad-Ausleihe – Ein Erfahrungsbericht

Um es gleich vorweg zu sagen: Ich fahre gern mit dem Rad – bei schönem Wetter deutlich lieber mit dem Rad als mit der Straßenbahn. Da es nicht unbedingt mein eigenes Fahrrad sein muss und dieses oft auf dem Nachhauseweg nicht zur Verfügung steht, kommt mir das Angebot der Kölner Verkehrsbetriebe KVB sehr entgegen: Mit meinem KVB-Abo-Ticket kann ich jederzeit ein Rad der in Leipzig beheimateten Nextbike GmbH ausleihen und muss in der ersten halben Stunde nichts dafür bezahlen. Im Sommer mache und machte ich das oft. Wie oft?

Nun, da beginnt das Problem: Ein Blick in meinen Nextbike-Account auf der Webseite zeigt mir in einer langen Liste sämtliche Ausleihen seit meiner ersten Anmeldung 2015. Da steht zum Beispiel für einen Tag im Herbst 2015

„14:54:05 Rad 21649 bis 15:07:12 (Ottoplatz / Oplader Str. (Bahnhof Deutz))".

Diese Ausführlichkeit haben nicht alle Einträge, nur für das Jahr 2017 sind fast alle Fahrten außer mit den Zeitangaben auch mit Straßennamen versehen – wohlgemerkt: oft mit denen von Start- und End-Punkt. Die Datenschutzerklärung auf der Webseite erwähnt dies nicht, sondern spricht lediglich ungenau von weiteren Daten, und nennt „z. B. den Zeitpunkt der Ausleihe sowie den Rückgabezeitpunkt zu Abrechnungszwecken".

Ein angeforderter Auszug meiner personenbezogenen Daten enthält genau die im Web sichtbaren Fahrt-Angaben in Textform, nicht etwa als GPS-Koordinaten, und Nextbike ergänzte in einer erläuternden Mail: „Gemäß §§ 257 HGB, 147 Abs. 1 Nr. 4, Abs. 3 AO sind wir zu einer Speicherung der Rechnungsdaten für einen Zeitraum von zehn Jahren verpflichtet." Mich irritiert, dass auch die kostenlosen, weil von der KVB übernommenen, Fahrten „Rechnungsdaten" sind, die mir als Person mit Ortsangaben zugeordnet werden müssen. Eine Nachfrage beim Datenschutzbeauftragten von Nextbike ist anhängig, doch dazu später mehr.

Zu meinem ehrlichen Erfahrungsbericht gehört auch eine kurze Beschreibung des eher entmutigenden Ablaufs meines Auskunftsersuchens. Nach E-Mail-Anschreiben an die auf der Webseite genannte Mail-Adresse datenschutz@nextbike.de im Februar und April dieses Jahres und einem Postbrief im September 2020 wurde die Auskunft erst erteilt, als ich im Oktober schließlich per E-Mail eine 48-Stunden-Frist bis zur Einschaltung der Aufsichtsbehörde einräumte. Allerdings antwortete nicht der auf der Webseite genannte Datenschutzbeauftragte, sondern jemand aus der Abteilung „Information Security Management". Seine Erklärung: „In diesem Jahr haben wir unsere Prozesse bezogen auf den Daten-

schutz erheblich umgestellt. Daher kam es dazu, dass vereinzelt Anfragen nicht beantwortet wurden. Die Probleme haben wir aber mittlerweile abgestellt ...“ Außerdem arbeite man daran, die Dateneinsicht nach dem Login auf der Webseite „kundenfreundlicher, in erster Linie übersichtlicher“ darzustellen.

Also versuchte ich, wie oben erwähnt, eine Auskunft vom auf der Webseite mittlerweile namentlich genannten Datenschutzbeauftragten zu erhalten, der interessanterweise im „Öffentlichen Verfahrensverzeichnis“ als „Mit der Leitung der Datenverarbeitung beauftragte Person“ aufgeführt wird. Seine Antwort auf meine per E-Mail gestellte Frage, warum teils die Anfangs- und Endpunkte meiner Fahrten in der Rechnung aufgelistet werden, teils aber auch nicht, steht zum Redaktionsschluss noch aus. Vielleicht sind für solche kniffeligen E-Mail-Anfragen sieben Arbeitstage etwas arg knapp. Ich werde es in zwei und dann in weiteren fünf Monaten nochmal versuchen und gerne an dieser Stelle darüber berichten. Aus meiner Sicht jedenfalls scheint die „erhebliche“ Umstellung der „Prozesse bezogen auf den Datenschutz“ bei Nextbike noch nicht komplett abgeschlossen zu sein. Am besten sollte wohl doch die Aufsichtsbehörde eine Hilfestellung leisten.

Offener Brief an EU-Kommission:

Keine Vorratsdatenspeicherung in der EU!

vom 06.10.2020

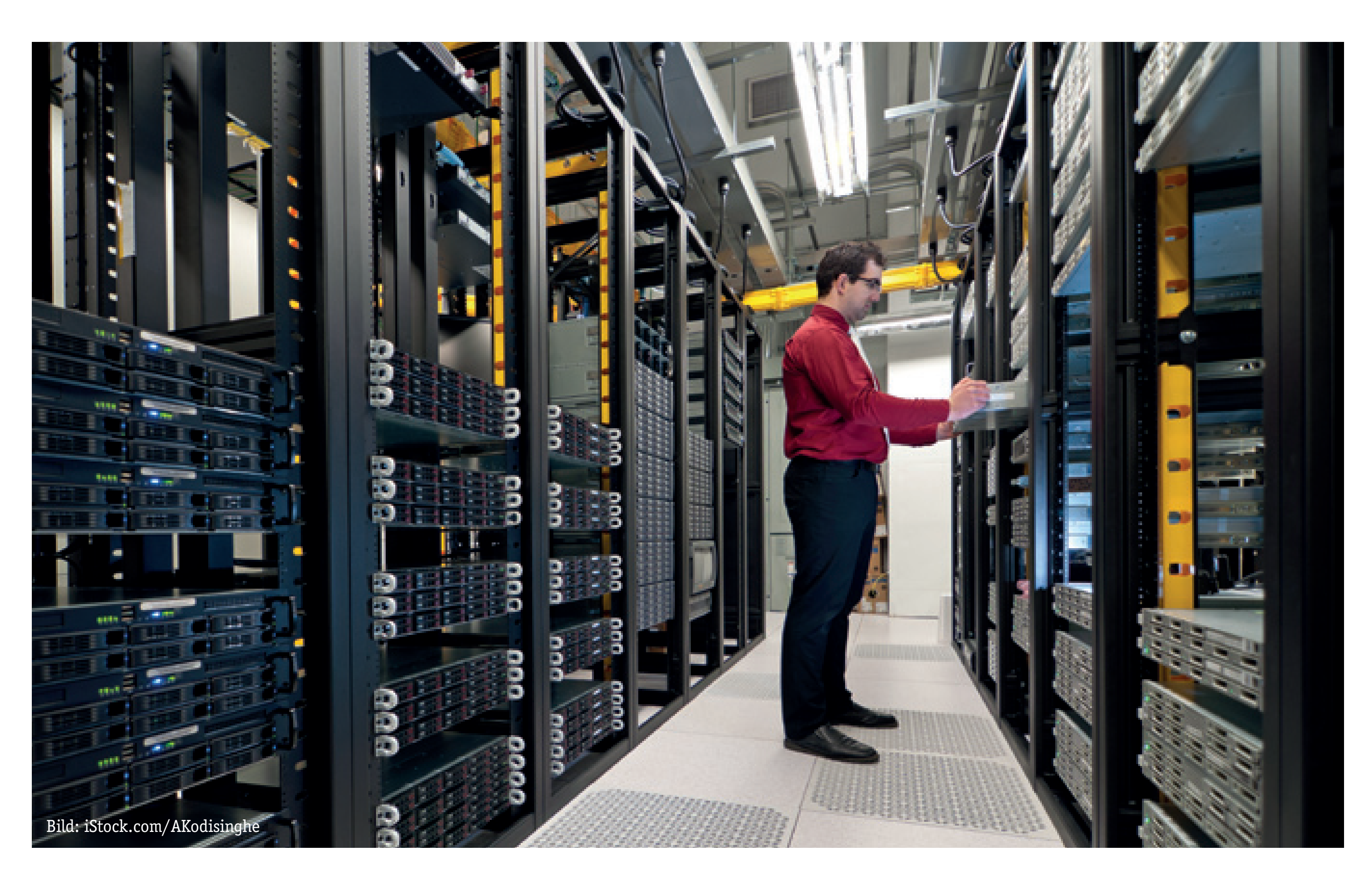


Bild: iStock.com/AKodisinghe

Sehr geehrte Frau Ylva Johansson, EU-Kommissarin für Inneres;

sehr geehrter Herr Thierry Breton, EU-Kommissar für den Binnenmarkt;

sehr geehrter Herr Didier Reynders, EU-Justizkommissar und

sehr geehrte Frau Margrethe Vestager, EU-Kommissarin für Wettbewerb und Digitales

Wir sind zutiefst beunruhigt über Erklärungen [1], dass die Kommission beabsichtigt die Notwendigkeit weiterer Maßnahmen zur Vorratsspeicherung von Kommunikationsdaten zu prüfen, sobald die Urteile in noch ausstehenden Fällen ergangen sind. Am 9. Dezember 2019 sagte Kommissarin Johansson [2]: „Ich denke schon, dass wir ein Gesetz für die Vorratsdatenspeicherung brauchen“. Eine Studie über „mögliche Lösungen für die Vorratsspeicherung von Daten“ wurde in Auftrag gegeben. Die deutsche Grundrechts- und Datenschutzorganisation Digitalcourage hält das Design der Studie [3] für voreingenommen, da es die Gefahren der Vorratsdatenspeicherung

in der Telekommunikation nicht berücksichtigt.

Die umfassende und anlasslose Vorratsspeicherung von Telekommunikationsdaten ist das am stärksten in die Privatsphäre eingreifende Instrument und möglicherweise die unbeliebteste Überwachungsmaßnahme, die jemals von der EU verabschiedet wurde. Die EU-Richtlinie zur Vorratsdatenspeicherung schrieb die umfassende Erfassung sensibler Daten zu sozialen Kontakten (einschließlich Geschäftskontakten), Bewegungsverhalten und Privatleben (z.B. Kontakte mit Ärzten, Rechtsanwälten, Betriebsräten, Psychologen, Notrufnummern usw.) von 500 Millionen Europäerinnen und Europäern vor, die keiner Straftat verdächtigt werden.

In seinem Urteil vom 8. April 2014 setzte der Europäische Gerichtshof (EuGH) die Richtlinie 2006/24 zur Vorratsdatenspeicherung außer Kraft, die Telekommunikationsunternehmen verpflichtet hatte Daten über die Kommunikation aller ihrer Kunden zu speichern. Sie ist aber in verschiedenen Mitgliedsstaaten der Europäischen Union noch immer in nationales Recht umgesetzt.

Wir sind der Überzeugung, dass eine derartig invasive Überwachung der gesamten Bevölkerung nicht akzeptabel ist. Mit einer Regelung zur Datenspeicherung werden sensible Informationen zu sozialen Kontakten (einschließlich Geschäftskontakten), Bewegungsverhalten und das Privatleben (z.B. Kontakte mit Ärzten, Rechtsanwälten, Betriebsräten, Psychologen, Helplines usw.) von Millionen von Europäerinnen und Europäern gesammelt, ohne Vorliegen von individuellen Verdachtsmomenten. Die umfassende und anlasslose Vorratsspeicherung von Telekommunikationsdaten hat sich in vielen Bereichen der Gesellschaft als schädlich erwiesen. Die Vorratsspeicherung von Telekommunikationsdaten untergräbt das Berufsgeheimnis, schafft die ständige Gefahr von Datenverlusten und Datenmissbrauch und hält die Bürger davon ab vertrauliche Kommunikation über elektronische Netze zu führen. Sie untergräbt den Schutz journalistischer Quellen und schwächt damit die Pressefreiheit. Insgesamt beschädigt sie die Grundlagen unserer offenen und demokratischen Gesellschaft. Da es in den meisten Ländern kein finanzielles Entschädigungssystem gibt, müssen die enormen Kosten einer Regelung zur Vorratsspeicherung von Telekommunikationsdaten von den Tausenden betroffenen Telekommunikationsanbietern getragen werden. Dies führt zu Preiserhöhungen und zur Einstellung von Diensten, wodurch die Verbraucher indirekt belastet werden.

Studien [4] belegen, dass bereits die ohne Vorratsdatenspeicherung verfügbaren Kommunikationsdaten zur effektiven Aufklärung von Straftaten ausreichen. Eine umfassende Vorratsdatenspeicherung hat sich in vielen Staaten Europas als überflüssig, schädlich oder sogar verfassungswidrig erwiesen, z.B. in Österreich, Belgien, Deutschland, Griechenland, Rumänien und Schweden. Diese Staaten verfolgen die Kriminalität ebenso effektiv mit der gezielten Sammlung von Verkehrsdaten, die für individuelle Ermittlungen benötigt werden, wie z.B. den im Übereinkommen des Europarats über Computerkriminalität vereinbarten Rechtsrahmen zur Sicherung gespeicherter Daten.

Wir argumentieren, dass das aktuelle deutsche Gesetz zur Vorratsdatenspeicherung nicht als Vorbild für die EU angesehen werden darf. Erstens sind verschiedene Verfassungsbeschwerden gegen das Gesetz anhängig und zweitens verfolgt das deutsche Gesetz den gleichen grundsätzlich riskanten Ansatz Daten über alle Bürgerinnen und Bürger kontinuierlich und ohne Rücksicht auf individuellen Verdacht, Bedrohung oder Bedarf zu erheben.

Es gibt keinen Beweis dafür, dass die Vorratsspeicherung von Telekommunikationsdaten einen verbesserten Schutz vor Kriminalität bietet. Auf der anderen Seite sehen wir, dass sie Milliarden von Euro kostet, die Privatsphäre Unschuldiger gefährdet, vertrauliche Kommunikation beeinträchtigt und den Weg für eine immer größere Massenanhäufung von Informationen über die gesamte Bevölkerung ebnet. Als Vertreter der Bürgerinnen und Bürger, der Medien, der Fachleute und der Industrie lehnen wir gemeinsam die generelle Speicherung von Telekommunikationsdaten ab. Wir fordern Sie dringend auf, keine Versuche zur Wiedereinführung der Vorratsdatenspeicherung von Telekommunikationsdaten zu unternehmen. Gleichzeitig appellieren wir an Sie Vertragsverletzungsverfahren einzuleiten, um sicherzustellen, dass die nationalen Gesetze zur Vorratsdatenspeicherung in allen betroffenen Mitgliedsstaaten aufgehoben werden. Darüber hinaus rufen wir Sie dazu auf sich für ein EU-weites Verbot genereller und anlassloser Vorratsdatenspeicherung einzusetzen, die die Aktivitäten von Menschen erfassen. Wir fordern Sie auf den europäischen Weg weiterzuentwickeln mit dem Ziel einer EU, die frei von invasiver Überwachung ist. Wir würden uns freuen die Angelegenheit mit Ihnen persönlich zu besprechen, zu einem für Sie passenden Termin. Mit freundlichen Grüßen

1 https://www.europarl.europa.eu/RegData/questions/reponses_qe/2020/000389/P9_RE(2020)000389_EN.pdf

2 https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/004385/P9_RE(2019)004385_EN.pdf

3 https://digitalcourage.de/blog/2020/data-retention-biased-study-by-the-eu-commission
https://digitalcourage.de/blog/2020/vorratsdatenspeicherung-einseitige-studie-der-eu-kommission

4 EDRi: Data Retention Booklet: https://edri.org/our-work/launch-of-data-retention-revisited-booklet/

Erstunterzeichner:

Access Now; ARTICLE 19, UK; Associação D3 - Defesa dos Direitos Digitais, Portugal; Association for Technology and Internet / Asociatia pentru Tehnologie si Internet (ApTI), Romania; Chaos Computer Club e.V., Germany; Citizen D/Državljan D, Slovenia; Dataskydd.net, Sweden; Datenschutzraum e.V., Germany; Deutsche Aidshilfe, Germany; Deutsche Vereinigung für Datenschutz (DVD) e.V., Germany; dieDatenschützer Rhein Main, Germany; Die Neue Richtervereinigung - Zusammenschluss von Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten e.V., Germany; Digitalcourage e.V., Germany; Digitale Gesellschaft, Germany; Digital Freedom (Digitale Freiheit e.V.), Germany; Digital Freedom and Rights Association / DFRI - Föreningen för digitala fri- och rättighjeter, Sweden; Digital Rights Ireland; Ire-

land; Dr. Thilo Weichert, Netzwerk Datenschutzexpertise, Germany; eco - Verband der Internetwirtschaft e.V., Germany; European Digital Rights (EDRi), EU-wide network; Electronic Frontier Finland, Finland; Electronic Frontier Foundation, U.S.A.; Electronic Frontier Norway, Norway; epicenter.works - Plattform Grundrechtspolitik, Austria; FREELENS e.V., Germany; Freifunk Hamburg, Germany; Forum Computer Professionals for Peace and Societal Responsibility, Germany / Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., FIfF, Germany; Hermes Center for Transparency and Digital Human Rights, Italy; Homo Digitalis, Greece; Internet Society, Bulgaria; Internet Society, German Chapter (ISOC.DE) e.V., Germany; IT-Political Association of Denmark (IT-Pol), Denmark; Iuridicum Remedium, z. s., Czech Republic; Komitee für Grundrechte und Demokratie, Germany; Mike O'Neill, Director of Baycloud Systems, UK; Panda Mery; quintessenz – Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter, Austria; Republikanischer Anwältinnen- und Anwälteverein e. V., Germany; Selbstbestimmt.Digital, Germany; Statewatch, UK; Vereinigung Demokratischer Juristinnen und Juristen e.V. (VDJ), Germany; Vrijschrift, Netherlands; Working Group on Data Retention (Arbeitskreis Vorratsdatenspeicherung), Germany; Xnet, Spain

Neue Richtervereinigung (NRV)

Zusammenschluss von Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten e.V. – Fachgruppe Verwaltungsrech. Pressemitteilung vom 18.05.2020

Kritik an der Auswertung von Datenträgern durch das BAMF hält an

Die im Juli 2017 eingeführte Befugnis, Datenträger von Asylsuchenden auszuwerten, soweit dies für die Feststellung der Identität und Staatsangehörigkeit erforderlich ist (§ 15a AsylG), unterlag schon im Gesetzgebungsverfahren verfassungsrechtlichen Bedenken. Darüber hinaus gibt die praktische Handhabung durch das Bundesamt für Flüchtlinge und Migration (BAMF) Anlass zur Sorge. Offenbar werden die Smartphones Geflüchteter massenhaft ausgelesen, die dabei gewonnenen Informationen führen aber kaum einmal zu tatsächlich relevanten Erkenntnissen für das Asylverfahren. Angesichts der verschwindend geringen Relevanz derartiger Zugriffe und der hohen Intensität der hiermit verbundenen Grundrechtseingriffe ist auch dies kritisch zu sehen.

Smartphones stellen heute ein elementares Instrument für die Teilhabe am sozialen, beruflichen und auch am Intimleben dar. Die hier gespeicherten Informationen gehören zu den denkbar sensibelsten Daten, die – in Summe – das alltägliche Leben praktisch vollständig digital abbilden können. Die Problematik liegt auf der Hand: Flüchtlinge tragen gerade in ihren Smartphones in aller Regel zahlreiche Privatkontakte, Konversationen, Fotos, kurz „ihr Leben und ihre Heimat" mit sich. Bei der Vorlage im Rahmen des Asylverfahrens könnte das BAMF auch die Standorthistorie oder die Sprache der auf dem Handy gespeicherten Textnachrichten analysieren. Das Auslesen und Auswerten dieser Daten ist ausgesprochen grundrechtssensibel. Dem trägt das deutsche und europäische Verfassungsrecht durch die Grundrechte auf Privatleben sowie Datenschutz Rechnung. Die gesetzlichen Voraussetzungen und die Notwendigkeit einer solchen Erhebung müssen deshalb im Einzelfall sorgfältig geprüft werden. Ein routinemäßiger Einsatz verbietet sich.

Dennoch ergaben Recherchen, dass das Verfahren jährlich zehntausendfach angewandt und zur Standardmaßnahme degradiert wird. Laut Berichterstattung über drei jüngst erhobene Klagen Betroffener sollen sich laut BAMF in 60% der Fälle keine zusätzlichen, für das Asylverfahren relevanten Erkenntnisse ergeben haben. In 38% der Fälle hätten die ausgewerteten Daten die Angaben des Geflüchteten bestätigt. In nur 2% der Fälle seien die Angaben widerlegt worden. Hinzu kommt, dass laut der Gesellschaft für Freiheitrechte (GFF), die die erwähnten Klagen begleitet, nur etwa 30% der durchgeführten Datenauswertungen überhaupt im Asylverfahren zu Rate gezogen werden. Steht beim Auslesen der Daten aber noch nicht fest, ob sie später auch genutzt werden, kommt dies einer Vorratsdatenspeicherung gleich.

Eine Überprüfung des Verfahrens, d.h. seiner Rechtsgrundlagen und praktischen Handhabung, ist dringend geboten. Eine Anfrage der Fachgruppe an den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI), der die Datenträgerauswertung überprüft, blieb Anfang Februar 2020 noch ohne Ergebnis, weil die Prüfung noch andauere. Einer ersten gerichtlichen Erörterung könnte die Rechtmäßigkeit der Datenverarbeitung jetzt anlässlich der vor den Verwaltungsgerichten Hannover, Berlin und Stuttgart eingeleiteten Klageverfahren unterzogen werden.

Die Fachgruppe beobachtet mit Sorge, dass Verfahrensneuerungen wie jetzt die Smartphoneanalyse wieder einmal an den Schwachen und Schwächsten der Gesellschaft erprobt werden. Es ist müßig daran zu erinnern: Die Grundrechte auf Privatleben und Datenschutz gelten unabhängig von Nationalität und Herkunft.

Werner Hülsmann

20. BigBrotherAwards-Verleihung



Laudatio von Dr. Thilo Weichert – Foto von Fabian Kurz, CC BY-SA 4.0

Die Veranstaltung

Dieses Jahr fand die 20. BigBrother-Awards-Verleihung in Bielefeld statt. Was ursprünglich als großes Jubiläumsfest im April dieses Jahres geplant war, wurde coronabedingt in den September verlegt und in einem kleinen, überschaubaren Rahmen durchgeführt. Verzichtet werden musste unter anderem auf „die rappelvollen Reihen im Publikum (...) und die anregenden Gespräche beim Sektempfang nach der Verleihung." Aber auch unter diesen Bedingungen war die Verleihung der „Oscars für Überwachung" eine beeindruckende Veranstaltung mit einem per Videobotschaft übermittelten Grußwort von Gerhard Baum (Bundesinnenminister von 1978 bis 1982).

Die PreisträgerInnen

Alle Laudationen zu den nachfolgend genannten PreisträgerInnen finden Sie auf https://bigbrotherawards.de/2020.

Kategorie „Mobilität"

Tesla, vertreten durch die Tesla Germany GmbH, München. Eine überarbeitete Version der Laudatio ist im Artikel „Tesla – Überwachungsmobil und Datenschleuder" von Thilo Weichert in dieser DANA-Ausgabe abgedruckt.

Kategorie „Behörden und Verwaltung"

In dieser Kategorie geht der BigBrotherAward 2020 an den Innenminister des Landes Brandenburg, Michael Stübgen, und seinen Vorgänger Karl-Heinz Schröter. „Prämiert" werden sie für die dauerhafte Speicherung von Autokennzeichen.

Kategorie „Bildung"

Den BigBrotherAward in der Kategorie „Bildung" erhalten die Firmen BrainCo und der Leibniz-Wissenschaftscampus Tübingen. Die Firma BrainCo wird für ihre EEG-Stirnbänder „ausgezeichnet", die mittels Gehirnstrommessung angeblich die Konzentration von SchülerInnen messen können. Leibniz-Wissenschaftscampus Tübingen erprobt eine ähnliche EEG-Technik kombiniert mit Eyetracking auch in Deutschland. „Das ist Dressur statt Bildung."

Kategorie „Politik"

Wegen ihrer rechtlichen und politischen Mitverantwortung für den völkerrechtswidrigen US-Drohnenkrieg erhält die Bundesregierung (CDU/CSU-SPD) den Negativpreis in der Kategorie „Politik". Dieser Drohnenkrieg wird über die Datenrelais- und Steuerungsstation der US-Militärbasis Ramstein/Pfalz abgewickelt wird.

Kategorie „Digitalisierung"

Die Verlegung der BigBrotherAward-Verleihung 2020 vom April in den Herbst führte zu einer weiteren Preisträgerin, die sich erst im Sommer „qualifiziert" hat: Weil sie wesentliche Dienste der Digitalen Bildungsplattform des Landes Baden-Württemberg von Microsoft betreiben lassen will, erhält die Bildungsministerin des Landes Baden-Württemberg, Susanne Eisenmann, den BigBrotherAward 2020 in der Kategorie „Digitalisierung". Die Laudation hierzu hat es im Nachgang sogar auszugsweise in den Bildungsausschuss des Ministeriums geschafft und wurde dort diskutiert.

Kategorie „Arbeitswelt"

Der BigBrotherAward 2020 in der Kategorie „Arbeitswelt" geht verdienterweise an die H&M Hennes & Mauritz B.V. & Co. KG (H&M) in Hamburg „für jahrelange, hinterhältige und rechtswidrige Verarbeitung von Beschäftigtendaten im H&M-Kundencenter in Nürnberg". Dort hat H&M im Rahmen von Pausengesprächen Daten über Krankheiten von MitarbeiterInnen gesammelt. Das fand auch die zuständige Datenschutzaufsichtsbehörde nicht lustig. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte gegen H&M ein Bußgeld in Höhe von 35,3 Millionen Euro wegen diesen Datenschutzverstößen[1].

Kategorie „Geschichtsvergessenheit"

Die Innenministerkonferenz der Bundesrepublik Deutschland (IMK) hat die Absicht, auf der Basis der Steuer-Identifikationsnummer eine lebenslang gültige Personenkennziffer einzuführen. Eine eindeutige Personenkennziffer widersprich nicht nur dem Grundgesetz. „Derartige Personenkennziffern wurden in den zwei Diktaturen auf deutschem Boden – im Nazideutschland und in der DDR – zur Erfassung, zur Repression bis hin zur Vernichtung genutzt". Für dieses Vorhaben erhält die IMK den BigBrotherAward 2020 in der Kategorie „Geschichtsvergessenheit".

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund/Europa

Mehr deutsche Behörden erhalten Zugriff auf SIS

Das Schengener Informationssystem (SIS), das bislang der Polizei vorbehalten war, wird für Tausende weiterer Behörden geöffnet. An das zentrale europäische Fahndungssystem werden auch Ausländerbehörden, Auswärtiges Amt, Botschaften und Zulassungsstellen für Fahr-und Flugzeuge sowie Schiffe angeschlossen. Im SIS schreiben Polizei, Zoll und Justiz aus EU-Staaten sowie Island, Schweiz, Norwegen und Liechtenstein Menschen zur Fahndung aus: Schwerverbrecher, Terrorverdächtige, jugendliche Ausreißer. Auch verschwundene und gestohlene Gegenstände wie Waffen oder Autos werden ins System eingespeist. Einreiseverbote werden im System gespeichert. Fingerabdrücke, Gesichtsbilder und DNA-Profile können im System hinterlegt werden. Deutschland setzt nun mehrere EU-Verordnungen um, um das SIS in seiner nächsten Stufe auszubauen.

Mit dem geplanten Umbau verschmelzen die Datenpools, auf die Polizei- und Migrationsbehörden zugreifen, weiter. Das Bundesamt für Migration und Flüchtlinge (BAMF) sowie alle Ausländerbehörden werden dem Bundesinnenministerium (BMI) zufolge an das SIS angebunden. Sie sollen das System für „ausländerrechtliche Ausschreibungen“ nutzen. Asylbewerber können sich im Gegensatz zu praktisch allen anderen Menschen in Deutschland nicht frei bewegen. Deshalb kann nicht nur nach ihnen gefahndet werden, wenn sie ausreisepflichtig sind, sondern auch, wenn sie etwa eine Woche lang nicht in ihrer Unterkunft auftauchen.

Gemäß den Antworten des BMI auf Anfragen der Linken-Fraktion können bald 2.000 Behörden das System nutzen. Wie viele Personen damit an die sensiblen Daten kommen können, wird nicht verraten. Das Kraftfahrtbundesamt und über dieses die Zulassungsstellen für Kfz, Luftfahrtbundesamt, Wasser- und Schifffahrtsämter sollen ebenfalls angebunden werden, von 2021 an auch lokale Waffenbehörden. 94 Mitarbeiter, unter anderem aus Bundespolizeibehörden, BAMF und externen Unternehmen, arbeiteten daran, die vielen Behörden im SIS zusammenzuschließen.

Der Bundestagsabgeordnete Andrej Hunko (Linke) sieht den Ausbau von Datenbanken der Sicherheitsbehörden kritisch: „Aus Deutschland kennen wir nicht endende Berichte, dass Polizeidatenbanken für Voyeurismus, Stalking oder rechtsextreme Umtriebe zweckentfremdet werden. Ich stehe der geplanten Ausweitung deshalb äußerst skeptisch gegenüber. Mich besorgt auch der Zuwachs nichtpolizeilicher Behörden. Ich erwarte nicht nur mehr Suchläufe im SIS, sondern auch mehr Einträge zur Fahndung. Dies mag in vielen Fällen sinnvoll erscheinen, öffnet aber Scheunentore für den Missbrauch.“ Tatsächlich hatten EU-Inspektoren 2017 festgestellt, dass Beamte aus Großbritannien illegale Kopien der SIS-Datenbank angefertigt hatten (Brühl, Fahnden mit der Superdatenbank, SZ 30.10.2020, 6; Europäische Union: Die Super-Fahndungsdatenbank kommt, www.suedeutsche.de 29.10.2020).

Bund

BMI-Referentenentwurf für Personenkennziffer

Nachdem sich die große Koalition auf Eckpunkte für einen virtuellen Zusammenschluss der Melderegister und zahlreicher anderer behördlicher Datenbanken geeinigt hat, wurde vom Bundesinnenministerium (BMI) ein Referentenentwurf zur „Einführung einer Identifikationsnummer in die öffentliche Verwaltung“ (Stand Juli 2020) vorgelegt, wonach die Steuer-ID zu einer allgemeinen Bürgernummer für alle möglichen Ämter erweitert werden soll. Mit der Identifikationsnummer sollen die mit dem Onlinezugangsgesetz (OZG) vorgesehenen E-Government-Dienste mithilfe der relevanten Verwaltungsregister von Bund und Ländern umgesetzt werden. Die Kennung soll gewährleisten, dass sogenannte Basisdaten natürlicher Personen „von einer dafür verantwortlichen Stelle auf Inkonsistenzen geprüft, verlässlich gepflegt, aktualisiert und bereitgestellt werden“.

Die Registermodernisierung soll über eine übergreifende Suchmaske erfolgen. Um den gewünschten Datensatz anhand grundlegender Informationen wie Name und Anschrift in unterschiedlichen Registern von Bund und Ländern finden zu können, soll die Personenkennziffer nötig sein. Dabei will das Ministerium Vorarbeiten der Innenministerkonferenz (IMK) entsprechend (DANA 1/2020, 48 f.) „auf die vorhandenen Strukturen der Steuer-Identifikationsnummer“ aufsetzen und diese „um die für ein registerübergreifendes Identitätsmanagement notwendigen Elemente“ ergänzen.

Nur eine eindeutige ID, „die in allen Registern gleichermaßen vorliegt“, ermögliche eine medienbruchfreie, verwaltungsübergreifende und nutzerfreundliche Kommunikation. Ohne ein solches Ordnungskriterium könne der Grundsatz „once only“ nicht umgesetzt werden, wonach die Bürger ihre Daten der Verwaltung nur einmal geben müssen. Dies entspreche auch dem Gebot der Datenminimierung. Um zu vermeiden, dass Profile erstellt werden, dürfe die ID selbst keine Rückschlüsse auf andere persönliche Informationen zulassen. Als zentrale Relaisstation soll das Bundesverwaltungsamt (BVA) dienen und dafür zur „Registermodernisierungsbehörde“ ausgebaut werden. Es soll beim Bundeszentralamt für Steuern (BZSt) gespeicherte Daten zur Steuer-ID im automatisierten Verfahren abrufen und im Sinne des OZG an registerführende sowie

andere öffentliche Stellen übermitteln dürfen. Der Transfer soll über eine Ende-zu-Ende-Verschlüsselung abgesichert werden.

Bei Datenabrufen prüfe die als „dritte Stelle" zwischengeschaltete Behörde automatisiert bei jedem Aufbau einer Verbindung anhand sicherer Authentifizierungsverfahren die Identität des abrufenden Amts, über die „kein Zweifel bestehen" dürfe. Näheres zum technischen Verfahren soll das Innenministerium per Verordnung festlegen können. Der Bundesdatenschutzbeauftragte soll die Behörde regelmäßig überprüfen können, das Gesetz soll nach drei Jahren mithilfe von „wissenschaftlichem Sachverstand" durch das Innenressort evaluiert werden. Derart verknüpft werden sollen so unter anderem Melderegister, das Ausländerzentralregister sowie Datenbanken etwa für Führerschein-, Waffen- oder eID-Kartenbesitzer. Dazu kämen etwa auch das Schuldner- und Anwaltsverzeichnis sowie Register für Wohngeld- und Bafög-Empfänger. Die vorgesehenen Basisdaten umfassen Informationen wie Namen, Geburtsort und -datum, Geschlecht, Anschriften, Tag des Ein- oder Auszugs sowie Staatsangehörigkeiten. Auch eine mögliche Auskunftssperre für besonders schützenswerte Personen soll vermerkt werden. Große Unterschiede zu den derzeit über Melderegister abrufbaren Merkmalen gibt es demnach nicht.

Aktuelle Basisdaten zu natürlichen Personen seien, so der Entwurf, ein zentrales Anliegen. Werde die Verwaltung digitalisiert, müsse im Interesse aller Beteiligten gewährleistet sein, dass Personenverwechslungen ausgeschlossen und vorhandene Datenbestände den Bürgern fehlerfrei zugeordnet werden könnten. Für die Transparenz gegenüber den Bürgern soll ein „Datencockpit" sorgen, das eine „einfache, transparente und zeitnahe Wahrnehmung der Betroffenenrechte" nach der Datenschutz-Grundverordnung (DSGVO) ermögliche.

Für Datenschützer ist ein allgemeines Personenkennzeichen ein rotes Tuch. Sie bemängeln seit Langem, dass die Steuer-ID entgegen ursprünglichen politischen Beteuerungen zunehmend in den verschiedensten Lebensbereichen verwendet wird. Der Bundesdatenschutzbeauftragte Ulrich Kelber lehnt den vorgesehenen Ansatz auch aus verfassungsrechtlichen Gründen ab. Es bestehe die Gefahr einer „vollständigen Registrierung und Katalogisierung der Persönlichkeit". Der Normenkontrollrat hatte in seiner Blaupause zur Registermodernisierung 2017 auf eine datenschutzfreundlichere Variante nach dem Vorbild Österreichs verwiesen.

Das BMI räumt ein, dass es um einen „Eingriff in das Recht auf informationelle Selbstbestimmung" der Bürger geht. Dieser sei aber „insgesamt verfassungsrechtlich gerechtfertigt, weil in der registerunterstützten und datenbankbasierten Verwaltung ein hohes Bedürfnis für eine eineindeutige Zuordnung von Datensätzen zu der jeweils richtigen Person besteht". Die einmaligen Kosten für den Aufbau einer vernetzten Registerstruktur schätzt das Haus von Horst Seehofer (CSU) auf etwa 915,7 Millionen Euro (Krempl, Vernetzte Register: Seehofer macht Ernst mit Steuer-ID als Bürgernummer, www.heise.de 25.08.2020, Kurzlink: https://heise.de/-4878923).

Bund

Quellen-TKÜ für Geheimdienste

Nach langem Ringen bekommt der Bundesinnenminister ein Gesetz, mit dem auch das Bundesamt für Verfassungsschutz (BfV) Trojaner einsetzen darf, um Verdächtige auszuspähen. Das Bundeskabinett hat am 21.10.2020 die Novelle des Verfassungsschutzgesetzes sowie weiterer Geheimdienstgesetze beschlossen. Damit sollen die deutschen Verfassungsschützer sowie der Militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) künftig Software zur Überwachung von Verdächtigen einsetzen dürfen, den so genannten Staatstrojaner. Polizeibehörden nutzen diese „Quellen-TKÜ" genannte Methode der Telekommunikationsüberwachung (TKÜ) bereits. In einem Statement aus seinem Ministerium nennt Bundesinnenminister Horst Seehofer das Gesetz einen „überfälligen Schritt im Kampf gegen Terroristen und militante Extremisten": „Wir brauchen einen Verfassungsschutz, der auch im digitalen Zeitalter sehen und hören kann. Nur so können wir den extremistischen Geschwüren in unserer Gesellschaft etwas entgegensetzen." Das Gesetz muss noch vom Bundestag gebilligt werden.

Ein Sprecher des SPD-geführten Bundesjustizministeriums sagte, es handele sich insgesamt um eine „maßvolle Kompetenzerweiterung" bei einer gleichzeitigen Stärkung der parlamentarischen Kontrolle, so wie im Koalitionsvertrag vorgesehen. Der vom Kabinett gebilligte Entwurf aus dem Bundesinnenministerium sieht auch einen erweiterten Austausch von Informationen zwischen dem MAD und den Verfassungsschutzbehörden vor. Das soll vor allem helfen, rechtsextreme Bundeswehrangehörige und Reservisten besser als bisher zu identifizieren.

Die Opposition warf der SPD vor, sich auf einen schlechten Deal eingelassen zu haben. Sie vermutet, die SPD habe dem Gesetz nach langem Ringen zugestimmt, um von der Union eine ebenfalls umstrittene Studie zu Rassismus in der Polizei zu bekommen. Der Grünen-Netzexperte Konstantin von Notz sagte: „Dieser Deal ist schlecht für unsere Bürgerrechte und geht direkt auf Kosten unserer Verfassung." Statt eine noch ausstehende Entscheidung des Bundesverfassungsgerichts zum Einsatz des Staatstrojaners bei der Polizei abzuwarten, weite die Regierung „das hochumstrittene Instrument" nun auch noch auf den Geheimdienstbereich aus.

Die Überwachung der klassischen Telekommunikation, also etwa des Telefons, ist seit Langem Teil des Repertoires des Inlandsgeheimdienstes, um Verfassungsfeinden nachzuspüren. Seit die Kommunikation sich vom Festnetztelefon über Handys hin zu Messengern verlagert hat, hilft diese Befugnis immer weniger. Nachrichten auf Whatsapp und in anderen Messenger-Diensten sind Ende-zu-Ende verschlüsselt. Kryptografie, die früher nur beim Militär und bei Geheimdiensten eine Rolle spielte, ist auf Smartphones jetzt für jedermann verfügbar: Whatsapp-Nachrichten etwa werden auf dem Telefon des Senders verschlüsselt, über die Leitungen von Vodafone, Telekom oder O2 fließt nur Buchstabensalat. Erst beim Empfänger wird die Nachricht wieder entschlüsselt. Ein Ableiten der Kommunikation an Internetknoten oder eine Nachfrage beim Netzbetreiber hilft also nicht mehr.

Der Staatstrojaner soll die durch Verschlüsselung für den Massenmarkt entstandene Informationslücke der Behörden schließen. Damit werden heimlich Programme auf die Telefone der Zielpersonen gespielt; dort werden die Nachrichten schon vor der Verschlüsselung abgegriffen und ausgeleitet. Das ist deutlich aufwändiger, als eine Telefonleitung abzuhören, aber potenziell auch deutlich mächtiger. Ist das Programm einmal auf dem Smartphone eines Ziels installiert, könnten die Verfassungsschützer nicht nur die gerade stattfindende Kommunikation sehen, sondern die gesamten auf dem Handy gespeicherten Daten.

Das Bundesinnenministerium hätte sich für die Novelle deshalb auch die sogenannte Online-Durchsuchung gewünscht – den Zugriff auf alle Daten auf den Telefonen. Die SPD kann sich auf die Fahnen schreiben, diesen tieferen Eingriff in die Privatsphäre verhindert zu haben. Ansehen dürfen Verfassungsschützer demnach lediglich Kommunikation ab dem Zeitpunkt der Anordnung der TKÜ. Doch auch das kann je nach Zeitpunkt der Aufspielung des Trojaners bereits weit in der Vergangenheit liegen. Kritiker fragen, wer (außer dem Gesetz) Verfassungsschützer daran hindert, dann mal einen Tag weiter in der Whatsapp-Historie zurückzublicken als eigentlich zulässig.

Durchgesetzt hat sich der Bundesinnenminister darin, dass die Netzbetreiber die Behörden bei der Installation der Schnüffel-Software unterstützen müssen. Andernfalls müsste der Verfassungsschutz die Telefone der Zielpersonen stehlen und gezielt präparieren. Jetzt sollen Mobilfunkanbieter verpflichtet werden, ein Update mit dem Schadprogramm zu schicken. Kontrollieren soll die TKÜ-Wünsche des BfV die schon bisher für Belange der Geheimdienste zuständige G-10-Kommission (benannt nach dem Grundgesetz-Artikel 10), die auf insgesamt zehn Mitglieder vergrößert werden soll. Zudem soll ein technischer Berater die Kommissionsmitglieder unterstützen.

Ulf Buermeyer, Vorsitzender der Gesellschaft für Freiheitsrechte (GFF), kritisierte den beschlossenen Gesetzentwurf deutlich. Zum einen sei die Kontrolle durch die G-10-Kommission deutlich löchriger als bei der TKÜ für die Polizeibehörden, bei der immer ein Richter zustimmen muss und bei der Ermittlungsergebnisse in Akten auftauchen. Zum anderen sei das Gesetz unnötig: Für Vorfeldbeobachtungen, wie sie der Verfassungsschutz klassischerweise durchführen soll, sei die TKÜ verfassungsrechtlich gar nicht zulässig. Beim Verdacht tatsächlicher Straftaten könne genauso gut die Polizei ermitteln. Die GFF denke deshalb bereits über eine Klage nach, sollte das Gesetz wie geplant in Kraft treten.

Der deutsche Staatstrojaner war bisher ein Flop. Seit einem Jahrzehnt basteln Behörden an immer neuen Varianten der Software, die Polizisten in Handys und Computer einschleusen, um Verdächtige auszuspähen. Manche Variante konnte nur die überholte Technik wie Skype überwachen, der zumindest intelligente Kriminelle längst abgeschworen hatten. Genutzt wurden Trojaner kaum. 2019 wurde bekannt, dass der Generalbundesanwalt in keinem einzigen seiner Terrorverfahren solche Software eingesetzt hatte. Dabei ist sie dem Bundesinnenminister zufolge angeblich die einzige Möglichkeit, Extremisten zu überführen. Sollten die Geheimdienste in ihrem Schattenreich mehr mit der Technik anfangen können als die Polizei, droht aber, dass die Überwachung in die Tiefe geht, da Ermittler in Chats auf Smartphones mehr abgreifen können als z.B. in einer aufgebrochenen Wohnung, etwa private Fotos oder intime Sprachnachrichten. Die Kontrolle der Dienste ist wegen deren Geheimniskrämerei viel schwieriger als die der Polizei. Parlament und Geheimdienstaufseher müssen deshalb genau hinsehen (Muth, Staatstrojaner für Verfassungsschützer, SZ 22.10.2020, 5; Brühl, Ein Flop macht Karriere, SZ 22.10.2020, 4; Kabinett will Geheimdiensten Zugriff auf Messenger-Nachrichten geben, www.heise.de 21.10.2020, Kurzlink: https://heise.de/-4934988).

Bund

Kanzleramts-Vorschläge zur BND-Kontrolle

Das Bundeskanzleramt hat einen 111-seitigen Gesetzentwurf zur Kontrolle des Bundesnachrichtendienstes (BND) vorgelegt, mit dem den Vorgaben des Bundesverfassungsgerichts (BVerfG) entsprochen werden soll. Im Zentrum des Vorschlags steht ein „Unabhängiger Kontrollrat". In Deutschland wird der Begriff „Kontrollrat" bisher assoziiert mit dem Gremium der Siegermächte. Dieser war nach dem Ende des Zweiten Weltkrieges als „Alliierter Kontrollrat" die oberste Besatzungsbehörde, die den Ausstieg des Landes aus dem Nationalsozialismus kontrollierte.

Nach dem Willen des Kanzleramts soll es von Januar 2022 an den Kontrollrat als oberste Bundesbehörde geben, in dem sechs Bundesrichter und Bundesanwälte darüber wachen sollen, dass der BND bei seinen weltweiten Abhöraktionen streng nach Recht und Gesetz handelt. Sieben Jahre nach den Enthüllungen des Whistleblowers Edward Snowden hat das Kanzleramt am 26.09.2020 den Gesetzentwurf in die sogenannte Ressortabstimmung gegeben. Das Kabinett beschließt daraufhin den Entwurf und legt ihn dem Parlament zur Debatte und Abstimmung vor.

Die Änderung des BND-Gesetzes ist notwendig, weil die Karlsruher Verfassungsrichter die Regierung dazu zwangen. In einem Urteil vom 19.05.2020 hatte das BVerfG entschieden, dass die bis dahin geltende Praxis, Ausländer im Ausland ohne jede Einschränkung abhören zu können, nicht mit dem Grundgesetz (GG) zu vereinbaren sei (Az. 1 BvR 2835/17; DANA 3/2020, 202 ff.). Die rechtsstaatlichen Kontrollen des Dienstes seien insgesamt viel zu halbherzig. Zu Unrecht ziehe sich der BND etwa auf das Argument zurück, seine Absprachen mit Diensten wie dem US-Abhörgiganten NSA seien zu geheim, um sie je Richtern zu zeigen. Rechtsstaatliche Sicherungen und nachvollziehbare Begründungen seien gefordert. Dies müsse unabhängig überwacht werden. Seither brüteten Regierungsjuristen und Experten der beim BND für das Abhörgeschäft zuständigen Abteilung „Technische Aufklärung" über dem Urteil. Dass es auf 145 Seiten mit insgesamt 331 Randnummern detailliert ist, machte die Spielräume für das Gesetz eng und schafft Klarheit, was geht und was nicht mehr geht.

Das Kanzleramt versucht nun, den Vorgaben aus Karlsruhe zu entsprechen: Der neue „Unabhängige Kontrollrat" soll

sich alles ansehen dürfen, was der BND weltweit unternimmt. Er soll größere Überwachungsaktionen wie die „strategische" Aufklärung, das heißt die verdachtsunabhängige Durchsuchung kompletter Telefonnetze, genehmigen müssen ebenso wie kleinere Überwachungsmaßnahmen. Er soll alle vom BND verwendeten Suchbegriffe prüfen dürfen, selbst wenn diese vom US-Geheimdienst NSA stammen.

All das soll zwar unter größter Geheimhaltung ablaufen. Für die Mitglieder des Kontrollrats gilt absolute Verschwiegenheit. Aber die sechs Juristen sollen intern ganz unabhängig arbeiten und entscheiden können. Vier von ihnen sollen Bundesrichter, zwei Bundesanwälte sein. Gemeinsam sollen sie zwei dreiköpfige „Kammern" bilden und einen fünfköpfigen „Senat". Gesucht werden juristische Fachleute, die überparteilich Anerkennung finden: Die Präsidentin des Bundesgerichtshofs soll sie nominieren, das Parlamentarische Kontrollgremium des Bundestages dann für je sechs Jahre wählen, das Bundeskabinett die Personalie nur noch abnicken. Die Regierung versichert, dies sei eine reine Formalie. Auch Richter am Bundesgerichtshof müssten schließlich offiziell vom Kabinett ernannt werden, ohne dass dies ihre Unabhängigkeit schmälere. Die Mitglieder des Kontrollrats sollen künftig von 25 Mitarbeitern unterstützt werden. Auch dies folgt einer ziemlich genauen Vorgabe des Bundesverfassungsgerichts. Damit soll wirkliche Schlagkraft entstehen. Bislang gab es nur ein aus drei Juristen bestehendes „Unabhängiges Gremium" mit Sitz in Karlsruhe, um die gesamte strategische Aufklärung des BND zu kontrollieren. Ein größeres Zugeständnis hatte die Bundesregierung den BND-Kritikern bei der letzten BND-Reform 2016 nicht machen wollen. Zudem hatten diese drei Juristen ihre Aufgabe nur im Nebenamt wahrgenommen.

Der Entwurf regelt auch die Online-Durchsuchung durch den BND im Ausland, also die Durchsuchung von Smartphones und Laptops mithilfe von Trojanersoftware. Die Methode wird in der SPD und der Opposition teils sehr kritisch gesehen. Zugleich wird eine gerichtliche Kontrolle eingeführt, die es in dieser Intensität noch nirgends gibt: Bevor der BND im Ausland ein Handy ausspioniert, muss er künftig immer erst die Genehmigung des Kontrollrats einholen. Selbst in Eilfällen muss zumindest ein Einzelrichter dort entscheiden.

Ein Streitpunkt betrifft noch die Frage, wer dem BND künftig auf die Finger schauen soll, ob er sich an die Entscheidungen des Kontrollrats auch wirklich hält. Das ist eine Aufgabe nicht für Juristen, sondern für Informatiker. Der Bundesdatenschutzbeauftragte (BfDI) Ulrich Kelber (SPD) würde das gern übernehmen. In seiner Behörde gibt es technische Fachleute, die sich in die Rechner des BND einklinken und dort stichprobenhaft die Abläufe überprüfen könnten. Das BVerfG hat diese Arbeit in seinem Urteil als „administrative Rechtskontrolle" bezeichnet. Das Kanzleramt sieht offenbar Probleme, wenn Mitarbeiter des Datenschutzbeauftragten mit ins Spiel kommen: Vor allem ausländische Nachrichtendienste könnten befürchten, dass die unbedingte Vertraulichkeit nicht gewährleistet bleibt. Der BfDI kontrolliert schon bisher den BND, ohne dass Indiskretionen bekannt geworden sind. Der Gesetzentwurf des Kanzleramts schlägt stattdessen vor, dass der Kontrollrat selbst Informatiker einstellt. Er werde auch schlagkräftiger sein, wenn alle, auch die technischen, Kompetenzen in seiner Hand gebündelt statt schon wieder zersplittert würden.

Die Karlsruher Richter haben besonders darauf hingewiesen, dass die Pressefreiheit ohne den Schutz von Informanten leerlaufen würde. Deshalb ist „ein gezieltes Eindringen in solche schutzwürdige Vertraulichkeitsbeziehungen" von Journalisten künftig nur noch mit besonders gewichtiger Begründung erlaubt. Die Überwachung von Journalisten wird im Gesetzentwurf nun zwar stark eingeschränkt, ist aber weiter nicht vollständig unmöglich. Im Ausnahmefall und zur Abwehr „schwerwiegender Gefahren" für die außenpolitischen Interessen der Bundesrepublik kann die vertrauliche Kommunikation von ausländischen Journalisten im Ausland belauscht werden. Ob diese Umsetzung des Urteils des BVerfG den Verbänden wie Reporter ohne Grenzen oder der Gesellschaft für Freiheitsrechte, die das BVerfG-Urteil erstritten, ausreichen wird, wird sich zeigen. Sie sollen schon bald zu dem Entwurf angehört werden.

Der Fraktionsvize der Grünen, Konstantin von Notz, begrüßte, dass die Regierung „sich auf den Weg macht" die Überwachung der elektronischen Kommunikation im Ausland „endlich rechtsstaatlich auszugestalten". Der FDP-Abgeordnete Stephan Thomae sprach ebenfalls von einem Fortschritt, wandte aber ein, dass die Bundesregierung die Chance verpasse gleich „die Nachrichtendienstkontrolle insgesamt neu zu ordnen". Der Fraktionsvize der Linken, André Hahn, kritisierte, durch dieses neue Gremium werde insgesamt ein Stück Kontrollmacht vom Parlament weg verlagert (Mascolo/Steinke, Spione unter Beobachtung, SZ 28.09.2020, 5; Lob und Kritik für BND-Gesetz, SZ 29.09.2020, 6).

Bund

Anti-Morphing und Fingerabdrücke künftig im Personalausweis

Am 26.10.2020 wurde im Innenausschuss des Bundestags im Rahmen einer Expertenanhörung der Entwurf für ein „Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen" erörtert. Der Entwurf sieht vor, dass beim Personalausweis ab August 2021 die Abdrücke der beiden Zeigefinger verpflichtend aufgenommen werden. Durch Regelungen zur Erstellung der Lichtbilder im Ausweis soll zudem das Morphing verhindert werden, also das Erfassen von gefälschten biometrischen Fotos. Die Bundesregierung wies darauf hin, dass Kriminelle digitale Passbilder von bis zu sieben Personen mit einer Morphing-Software zu einem neuen Passbild verschmelzen könnten und dieses dann von mehreren Personen verwendet werden könne. In der Anhörung im Innenausschuss sagte der grüne Innenpolitiker Konstantin von Notz, ein solcher Missbrauch sei bisher nur in wenigen einstelligen Fällen bekannt geworden. Die Lichtbildmanipulation wollte die Bundesregierung dadurch erschweren, dass Passbilder nur noch unter der Aufsicht von Beamten der Passbehörde gemacht werden. Den Fotostudios drohte

damit ein erheblicher Marktanteil wegzubrechen. Nach Protesten wurde der Gesetzentwurf dahin gehend verändert, dass die über 6.000 Pass- und Ausweisbehörden mit Kameras und Fotoautomaten ausgerüstet werden. Bürger können aber weiterhin Passfotos von freien Fotografen verwenden, die das Bild dann elektronisch über einen sicheren Kanal an die Behörde übermitteln müssen.

Neu vorgesehen ist weiterhin, dass Bürger den linken und den rechten Zeigefinger für den Personalausweis verpflichtend erfassen lassen. Bisher gibt es eine Speicherpflicht von Fingerabdrücken seit 2007 nur in Reisepässen, beim Personalausweis war diese Speicherung freiwillig. Rund 40 % der Bürger gaben bislang ihre Fingerabdrücke her. Die Fingerabdruckdaten sollen künftig im Chip des Personalausweises verschlüsselt gespeichert werden und bei Zweifeln am Foto zur Identitätskontrolle genutzt werden. Eine Speicherung in Dateien ist nicht erlaubt. Die Behörde muss die Datei mit dem Fingerabdruck an dem Tag löschen, an dem der Bürger seinen neuen Ausweis abholt.

Die Anhörung im Innenausschuss zeigte einige Kritikpunkte an dem Vorhaben auf. Friedemann Ebelt von der Bürgerrechtsorganisation Digitalcourage sieht in der Erfassung des Fingerabdrucks einen „Generalverdacht gegen Bürgerinnen und Bürger“. Aus seiner Sicht ist das Vorhaben unverhältnismäßig, da es nur in seltenen Einzelfällen begründete Zweifel am Lichtbild gibt. Aus Sicht von Digitalcourage ist die Erfassung der Fingerabdrücke nicht nötig, um die Fälschungs- und Manipulationssicherheit der Personalausweise zu erhöhen: „Die geplante Fingerabdruckpflicht hat im Grundgedanken nichts mit der Freizügigkeit der Bürger und Bürgerinnen zu tun, wie ein von der Bundesregierung angeführtes Argument behauptet. Sondern es ist eine Pflicht, ein Zwang, also Unfreiheit.“ Ebelt vermutet, dass mit den Fingerabdrücken vor allem eine zeitlich schnellere Überprüfung der Identität möglich gemacht werden solle.

Der Datenschutzsachverständige Thilo Weichert wies darauf hin, dass der Zweck zwar die unmittelbare Identitätsfeststellung sei. Doch sei auch ein Fahndungsabgleich mit den im Personalausweis gespeicherten Fingerabdrücken möglich, weil das Gesetz dies nicht ausdrücklich verbiete. Weichert warnte davor, dass mit Erfassungsgeräten zur Fingerabdruckverifizierung eine unangemessene Überwachungsinfrastruktur aufgebaut wird. Weichert schlug vor, statt des oft genutzten Zeigefingers den Ringfinger oder den kleinen Finger zur Speicherung zu nutzen, da diese weniger oft zum Beispiel auf Gläsern oder anderen Gegenständen hinterlassen würden und von Kriminellen für ihre Zwecke genutzt werden könnten. Zwar ist gemäß der Praxis der Internationalen Zivilluftfahrt-Organisation (ICAO) die Erfassung des Zeigefingers in internationalen Ausweisdokumenten wie Pässen üblich, doch maßgeblich für eine nationale Gesetzgebung sind deren Standards nach Auffassung Weicherts nicht. Weichert machte außerdem die Abgeordneten darauf aufmerksam, dass eine digitale Erfassung und Speicherung der Fingerabdrücke langfristig den Fingerabdruck für kriminalistische Zwecke entwerten könnte, falls die Daten etwa aus unzureichend gesicherten Systemen entwendet und von Kriminellen missbraucht würden.

Der IT-Experte Christoph Busch von der Hochschule Darmstadt wies darauf hin, dass bei der Identitätskontrolle ein In-sich-Abgleich des Fingers mit den auf dem Chip gespeicherten Daten stattfinde. Weichert erläuterte, dass die einmal digital erfassten Daten an andere Stellen weitergereicht werden können. Es sei zu erwarten, dass die Erfassung durch den massenhaften Einsatz von Fast-ID-Geräten im Laufe der Zeit zunehme. Das Fast-ID-Verfahren macht es möglich, einen Fingerabdruck innerhalb kurzer Zeit abzugleichen, so dass eine Person direkt vor Ort überprüft werden kann.

In der Anhörung nahm außerdem die Diskussion kartellrechtlicher Fragen einen breiten Raum ein. So ging es darum, ob private Anbieter durch die Vorrangstellung der Bundesdruckerei verdrängt werden würden. Die Bundesdruckerei soll zur einzigen Lieferantin für Geräte zur biometrischen Bilderfassung in den Kommunen bestimmt werden. Dies bezeichneten die Sachverständigen Georg Borges von Universität des Saarlandes und der IT-Sicherheitsexperte Roland Appel als verfassungsrechtlich problematisch (Schulzki-Haddouti, Der Generalverdacht, VDI-Nachrichten 30.10.2020, 18).

Bund

Löschungsfristen im Führungszeugnis bei Kindesmissbrauch werden hinterfragt

Der CSU-Landesgruppenchef Alexander Dobrindt will durch einen lebenslangen Eintrag im erweiterten Führungszeugnis erreichen, dass Verurteilte nie wieder beruflichen oder ehrenamtlichen Umgang mit Kindern haben können. Es müsse dafür gesorgt werden, dass ein solches Urteil „dauerhaft, lebenslang in das erweiterte Führungszeugnis eingetragen wird. Und nicht nur begrenzt auf zehn Jahre. Wer sich an den Schwächsten unserer Gesellschaft vergeht, der darf auch nie wieder beruflich oder ehrenamtlich Umgang mit Kindern haben.“ Im Februar 2020 hatten die Bundesländer Nordrhein-Westfalen, Baden-Württemberg, Bayern und das Saarland über den Bundesrat eine Streichung der Löschungsfristen eingebracht.

Opfervereine weisen immer wieder darauf hin, wie wichtig der Eintrag „sexueller Kindesmissbrauch“ im erweiterten Führungszeugnis sei und fordern eine Aufhebung der Löschfrist. Die Vorsitzende von Zartbitter, Ursula Enders, erinnerte daran, dass sie und ihre Kollegen schon in den 90er Jahren „alle im Bundestag“ deswegen angeschrieben hätten. Bei Kindesmissbrauch sei der Resozialisierung der Täter Vorrang vor den Belangen der Opfer gegeben worden. Seit langem wisse man aber, dass Tätertherapien bei Erwachsenen nur begrenzt erfolgreich seien und dass der „Erfolg“ lediglich darin bestehe, dass der Täter eine positive Einschätzung über sich selbst abgebe. Bei jugendlichen Missbrauchstätern sei dies anders, da hätten vor allem Gruppentherapien große Erfolgsaussichten. Deshalb plädiert auch Enders für eine Beibehaltung der Löschungsmöglichkeit bei Jugendlichen.

Laut Enders ist es eine „klassische Täterstrategie“, in pädagogische Arbeitsfelder zu gehen: „Wir erleben sehr

häufig, dass verurteilte Missbrauchstäter immer wieder in Vereinen oder anderen Einrichtungen, die mit Kindern und Jugendlichen arbeiten, auftauchen.“ Ein Problem sei, dass nicht alle Einrichtungen darauf vorbereitet seien. Private Einrichtungen wie Tanz- oder Musikschulen oder Anbieter von Selbstverteidigungskursen ließen sich das Führungszeugnis oft gar nicht vorlegen. Enders hält es daher für unabdingbar, eine Pflicht zur Vorlage einzuführen.

Dobrindt begrüßte zudem, dass die Justizministerin Christine Lambrecht (SPD) ihren Widerstand aufgegeben hat, das Strafmaß bei Kindesmissbrauch deutlich zu verschärfen. Es sei auch „richtig, dass wir endlich zu einer Einstufung als Verbrechen kommen und nicht mehr als Vergehen“. Die CSU wolle aber über diese Vorschläge hinausgehen.

Der Missbrauchsbeauftragte Johannes-Wilhelm Rörig warnte vor einem Nachlassen der öffentlichen Aufmerksamkeit für das Thema. Lambrechts Pläne zur Strafverschärfung halte er zwar für richtig und für ein „wichtiges Signal für Betroffene“. Aber allein mit höheren Strafen „verhindern wir Missbrauch nicht“. Es wäre deshalb ein „Riesenfehler“, die Debatte jetzt zu beenden. Strafverschärfungen hielten keinen Sexualstraftäter ab, „der Kinder vergewaltigt, foltert und dabei filmt“. Viel entscheidender sei es, das Entdeckungsrisiko für Missbrauchstäter zu erhöhen. Dies lasse sich wie in Nordrhein-Westfalen durch verbesserte Aufklärungs- und Präventionsarbeit und bessere polizeiliche Ermittlungsmöglichkeiten erreichen. Zentral sei auch eine enge Zusammenarbeit aller Behörden, die dem Kindeswohl dienten, besonders zwischen den Jugendämtern und den Familiengerichten. In Bezug auf den Vorschlag zum erweiterten Führungszeugnis warnte Rörig vor zu viel Optimismus. Fakt sei, dass „das erweiterte Führungszeugnis nur vor bereits verurteilten Sexualtätern schützen“ könne. „Die Mehrzahl der Täter ist aber weder entdeckt noch verurteilt.“ Zudem müsse bei jugendlichen Missbrauchstätern eine Einschränkung gemacht werden. Für sie dürfe der lebenslange Eintrag nicht gelten: „Da melde ich einen Vorbehalt an.“ Bei Jugendlichen könne man pädagogisch und therapeutisch besser nachsteuern.

Ein Sprecher des Justizministerium erklärte zu den Forderungen: „Die Ministerin ist offen für die weitere Diskussion über eine noch stärkere Ausweitung der Fristen und für fachlich fundierte Argumente im Gesetzgebungsverfahren.“ Er verwies aber auch auf das „grundrechtlich verankerte Interesse an der Resozialisierung“ von Tätern. Nach dem im Ministerium bearbeiteten Gesetzentwurf, in dem es um Strafverschärfungen, Strafverfolgung und Prävention geht, würden sich „zwangsläufig längere Aufnahmefristen in das erweiterte Führungszeugnis ergeben“. Auch bei Verurteilungen zu weniger als einem Jahr soll die Eintragung ins Führungszeugnis von drei auf zehn Jahre „erheblich verlängert“ werden (CSU will Kindesmissbrauch lebenslang im Führungszeugnis vermerken, www.zeit.de 13.07.2020; Rattenhuber, Lebenslang, zum Schutz der Kinder, SZ 14.07.2020, 6; Lebenslanger Eintrag im Führungszeugnis, Der Spiegel Nr. 30 v. 18.07.2020, 18).

Bund

BMJV plant strafprozessuales Kfz-Kennzeichen-Scanning

Gemäß einem veröffentlichten Referentenentwurf zur „Fortentwicklung der Strafprozessordnung“ (StPO) will das Bundesjustizministerium (BMJV) eine einheitliche Rechtsgrundlage schaffen, auf der die Polizei die automatisierten Kennzeichenlesesysteme (AKLS) im öffentlichen Verkehrsraum zu Fahndungszwecken nutzen kann. Gemäß dem geplanten § 163g StPO sollen Ordnungshüter „an bestimmten Stellen im öffentlichen Verkehrsraum“ ohne das Wissen der betroffenen Personen „amtliche Kennzeichen von Kraftfahrzeugen sowie Ort, Datum, Uhrzeit und Fahrtrichtung durch den Einsatz technischer Mittel automatisch“ erheben dürfen. Es müssen demnach „zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat von erheblicher Bedeutung begangen worden ist“. Zugleich soll die Annahme gerechtfertigt sein, dass so der Aufenthaltsort des Beschuldigten ermittelt werden kann.

Das Ministerium hofft damit, eine „klare Zweckbindung der Maßnahme“ zu kodifizieren. Schon mit dem Verweis auf Delikte von „erheblicher Bedeutung“ verwendet es aber einen weitgehend unbestimmten Rechtsbegriff. Eine solche Straftat liegt laut dem Bundesverfassungsgericht vor, „wenn sie mindestens der mittleren Kriminalität zuzurechnen ist, den Rechtsfrieden empfindlich stört und geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen“.

Meist handelt es sich Juristen zufolge um gewerbs-, gewohnheits-, serien- oder bandenmäßig oder anders organisierte Taten. Als Beispiele gelten neben Delikten, die besonders schutzwürdige Rechtsgüter wie Leib, Leben und Freiheit der Person sowie den Bestand und die Sicherheit des Bundes und der Länder betreffen, auch Betrugsfälle, Drogenkriminalität oder das Verbreiten von Darstellungen sexuellen Kindesmissbrauchs.

Die Daten dürfen laut dem Entwurf nur vorübergehend und nicht flächendeckend erhoben werden. Eine ausdrückliche und pauschal geltende Höchstfrist sei nicht nötig. Die erhobenen amtlichen Kfz-Nummernschilder dürften automatisch abgeglichen werden mit Halterdaten von Autos, die auf den Beschuldigten oder Kontaktpersonen zugelassen sind oder von diesen genutzt werden. Bedingung soll sein, dass die „Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre“. Das Kennzeichen müsse unverzüglich automatisch abgeglichen werden, nachdem die Daten erhoben worden seien. Bei einem Treffer sei genauso unverzüglich manuell zu überprüfen, ob die erhobenen Kennzeichen und Halterdaten übereinstimmen. Wenn kein Treffer vorliege oder dieser nicht bestätigt werden könne, seien die erhobenen Informationen „sofort und spurenlos zu löschen“.

Eine schriftliche Anordnung „der Staatsanwaltschaft oder ihrer Ermittlungsperson“ soll ausreichen, um die Scanner einzusetzen. Darin müssen laut dem Entwurf die Halterdaten der Verdächtigen und die „bestimmten Stellen“ der Überwachung genau bezeichnet werden. Die Anordnung sei zu befristen, ein Richtervorbehalt aber

nicht angezeigt. AKLS ermöglichten es, so das BMJV, „über einen bestimmten Zeitraum hinweg an überwachten Kontrollpunkten vor allem von Fernstraßen sämtliche passierende Fahrzeuge abzulichten, deren amtliche Kennzeichen durch eine Software auszulesen und sie mit Halterdaten von Kraftfahrzeugen abzugleichen". Dabei gelte es, die Rechte der Betroffenen durch klare Anordnungs- und Verfahrensvoraussetzungen zu schützen und die vom Bundesverfassungsgericht in jüngster Zeit aufgestellten Vorgaben zu berücksichtigen. Bundesjustizministerin Christine Lambrecht (SPD) erklärte, ihr gehe es darum eine „Regelungslücke im Bereich der strafprozessualen Ermittlungsbefugnisse" zu schließen. Die Novelle greife zudem einen Beschluss der Justizministerkonferenz vom Juni 2019 auf.

In der Gesetzesbegründung wird aufgeführt, das Instrument werde in anderen Bereichen staatlicher Kontrolle bereits seit Längerem erfolgreich eingesetzt und sei dort auch bereichsspezifisch gesetzlich geregelt. So dienten AKLS im Straßenverkehrsrecht schon seit 2005 dazu, die Mautpflicht durchzusetzen. Seit 2019 würden sie genutzt, um zu kontrollieren, ob Dieselfahrverbotszonen eingehalten werden. Auch für die Gefahrenabwehr werde die automatische Kennzeichenerfassung schon seit vielen Jahren anlassbezogen – teils als offene, teils als verdeckte Maßnahme – polizeilich in zahlreichen Bundesländern verwendet. Dies sei aber mit erheblichen Rechtsunsicherheiten behaftet.

Bisher könne das Kennzeichen-Scanning allenfalls auf § 100h StPO gestützt werden. Dieser Paragraph bestimme aber nur allgemein, dass „auch ohne Wissen der betroffenen Personen außerhalb von Wohnungen Bildaufnahmen hergestellt werden dürfen", um den Aufenthaltsort eines Beschuldigten herauszufinden. Insbesondere der ständige Abgleich von aufgenommenen Bildelementen mit mehr oder weniger umfangreichen Dateibeständen werde damit nicht erlaubt. Vor allem in Brandenburg ist das Kennzeichen-Scanning daher umstritten und erhielt 2020 einen BigBrotherAward; eine Verfassungsbeschwerde ist anhängig.

Das BMJV räumt ein, dass „typischerweise Personen in sehr großer Anzahl betroffen" würden. Diese alle anschließend über den Grundrechtseingriff zu benachrichtigen, „erscheint praktisch undurchführbar" und sei verfassungsrechtlich auch nicht geboten. Informiert werden sollen daher nur diejenigen, die erheblich betroffen seien, also der Beschuldigte oder Kontaktpersonen (Krempl, StPO-Reform: Justizministerium will Kfz-Kennzeichen-Scanning ausweiten, www.heise.de 16.10.2020, Kurzlink: https://heise.de/-4931007).

Bund

Kelber droht bei elektronischer Patientenakte mit Gegenmaßnahmen

Der Bundesdatenschutzbeauftragte (BfDI) Ulrich Kelber kündigte beim Start der elektronischen Patientenakte im Jahr 2021 an, Warnungen vor unzureichendem Datenschutz an Millionen von Versicherten einzufordern. Er könne dem Gesetzgeber keine Vorgaben machen und keine Gesetze korrigieren: „Ich kann und muss aber einschreiten, wenn bei Stellen, die meiner Aufsicht unterliegen, Datenverarbeitungsvorgänge gegen geltende Datenschutzvorschriften verstoßen." Das Gesundheitsministerium erklärte, die Bundesregierung teile die Bedenken ausdrücklich nicht.

Kelber plant Warnungen und Anweisungen gegenüber 65 gesetzlichen Krankenkassen mit insgesamt 44,5 Millionen Versicherten, über die er die Datenschutzaufsicht hat. Dies zielt unter anderem darauf, dass die Kassen vorgegebene „Warntexte" an ihre Versicherten schicken müssen. Kelber hatte die Konsequenzen angekündigt, wenn ein vom Bundestag beschlossenes Patientendatenschutzgesetz (PDSG) für die E-Akten unverändert bleibt. Und dieses blieb am 18.09.2020 bei der abschließenden Billigung durch den Bundesrat unverändert. Das PDSG wurde am 19.10.2020 im Bundesgesetzblatt verkündet und trat tags darauf in Kraft.

E-Akten sollen allen Versicherten ab 01.01.2021 zur freiwilligen Nutzung angeboten werden und zum Beispiel Befunde, Röntgenbilder, Impfungen und Medikamentenpläne speichern. In der Kritik steht schon seit längerem, dass zum Start eine etwas „abgespeckte" Version bei den Zugriffsrechten vorgesehen ist. So können Patienten festlegen, welche Daten überhaupt in die E-Akte sollen und welcher Arzt sie sehen darf. Genauere Zugriffe je nach Arzt nur für einzelne Dokumente kommen aber erst Anfang 2022. Das zwinge Nutzer, so Kelber, zu einem „Alles oder Nichts". Ein Zahnarzt könne alle Befunde eines Psychiaters sehen. Die Opposition kritisierte das ebenfalls.

Kelber kündigte an, vor dem 01.01.2021 eine Warnung an die ihm unterstehenden Kassen zu senden, dass eine reine Gesetzes-Umsetzung „zu einem europarechtswidrigen, defizitären Zugriffsmanagement" führen würde: „Der nächste Schritt werden Anweisungen sein." Diese sollen die Kassen verpflichten, bis zum 31.12.2021 für eine Ausgestaltung des Zugriffsmanagements zu sorgen, die der europäischen Datenschutzgrundverordnung (DSGVO) entspricht. In der Zwischenzeit sollen sie Versicherten, die ihre digitale Akte freiwillig nutzen möchten, „einen vorgegebenen Warntext" zukommen lassen müssen.

Das Bundesgesundheitsministerium betonte, das Gesetz sei von den Verfassungsressorts für Justiz und Inneres umfassend geprüft worden. Die E-Akte sei eine freiwillige Anwendung. Über die Funktionsweise müssten die Kassen ihre Versicherten vorab umfassend informieren: „Die Versicherten behalten die Hoheit über ihre Daten." Dem Start am 01.01.2021 stünden die Ankündigungen des Datenschutzbeauftragten nicht entgegen. Minister Jens Spahn (CDU) will nach jahrelangem Gezerre um mehr Funktionen der elektronischen Gesundheitskarte Tempo bei der Digitalisierung machen. Die E-Akten sollen schrittweise mehr Funktionen bekommen und auch per Smartphone abrufbar sein.

Kelber will auch zunächst per Warnung an die Kassen mit Blick auf die IT-Sicherheit einschreiten. Nach dem 01.01.2021 will er sie dann anweisen, bis spätestens 30.04.2021 ein „hoch" sicheres Verfahren anzubieten, mit dem man sich für eine berechtigte Nutzung anmelden kann. Die vorgesehenen Authentifizierungsverfahren seien „aus Datenschutzsicht nicht ausreichend

sicher" und entsprächen nicht den DS-GVO-Vorgaben.

Kelber betonte, er unterstütze ausdrücklich die Digitalisierung des Gesundheitswesens: „Sie bietet riesige Chancen für uns alle." Dies müsse aber auf Grundlage der DSGVO geschehen. Er fordert „eine sichere elektronische Patientenakte für alle, bei der man seine Daten voll im Griff hat." Im aktuellen Fall sehe er, dass die gesetzlichen Krankenkassen in einer „besonderen Situation" seien: „Sie sollen die Gesetze umsetzen, setzen sich damit aber in Widerspruch zum europäischen Recht." Daher würde er sich ein festgeschriebenes Recht als Bundesdatenschutzbeauftragter wünschen, nationale Normen bei vermuteter Europarechtswidrigkeit dem Europäischen Gerichtshof (EuGH) vorlegen zu können (Der E-Patientenakte drohen Datenschutz-Warnungen, www.fr.de 16.09.2020).

Bundesweit

Corona-Gästelisten verursachen Probleme

Millionen Menschen hinterlassen seit Monaten ihre Daten in Bars, Restaurants und Biergärten. Dazu gibt es einen Witz: „Was haben Mickey Maus und Klaus Störtebecker gemeinsam? Antwort: Sie schätzen beide einen Bahnhofsimbiss in Kiel." Dort musste das Gesundheitsamt Kunden aufspüren, nachdem mehrere Angestellte positiv auf Sars-CoV-2 getestet worden waren. Jeder zehnte Gast hatte falsche Angaben hinterlassen. Den Imbissbetreibern war nicht aufgefallen, dass die Comicfigur und der Freibeuter wohl in Wirklichkeit anders heißen.

Ähnliche Erfahrungen machte das Gesundheitsamt in Berlin-Neukölln. Dort war es in einem Brauhaus zu Infektionen gekommen. Auf den Kontaktlisten tauchten Namen wie „Hildegard Prost" und „Farin Urlaub" auf. Insgesamt 41 der rund 350 Datensätze waren falsch oder unvollständig. Am Ende stellte sich heraus: 22 Menschen waren infiziert, mehr als 70 mussten in Quarantäne. Nicht ausgeschlossen ist, dass Infizierte wegen ihrer falschen Angaben nicht ermittelt werden konnten. Dem Brauhausbetreiber Steffen Brückner droht nun ein Verfahren wegen einer Ordnungswidrigkeit: „Wir haben jetzt den Schwarzen Peter." Dabei könne ihm niemand erklären, mit welchem Recht er die Daten seiner Kunden hätte überprüfen sollen. Er habe schließlich keine Befugnis, sich ihre Ausweise zeigen zu lassen. Der Hamburgische Datenschutzbeauftragte stellte fest, dass rund ein Drittel der Betriebe offen ausliegende und für Fremde einsehbare Listen verwendet.

Seit Mitte Mai 2020 werden unzählige Daten im ganzen Land erfasst: Namen, Telefonnummern, Anschriften, E-Mail-Adressen. Ende April war die „vollständige Kontaktverfolgung" von Corona-Infizierten in der Einigung von Bund und Ländern die Voraussetzung für weitere Öffnungsmaßnahmen. Datenschützer kritisierten von Anfang an die Praxis. Im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein war Anfang August bereits eine dreistellige Zahl von Beschwerden eingegangen, bis Mitte Juli waren es bei der Aufsichtsbehörde in Nordrhein-Westfalen immerhin 60. Das bayerische Landesamt für Datenschutzaufsicht berichtet bis dahin über mehr als 50 Eingaben.

In den meisten Fällen wurde moniert, dass die Daten auf Listen oder in Ringbüchern gesammelt wurden, so dass sie von anderen eingesehen werden konnten. Urlauber befürchteten, dass auf diese Weise Diebe leer stehende Wohnungen auskundschaften. Unternehmer nutzten die Möglichkeit, um Kundendatenbanken aufzubauen und Newsletter zu verschicken. Eine Bremerin klagte, dass ein Kellner versucht hatte, sie mit den Informationen privat zu kontaktieren.

Die Polizeien in Bayern, Hamburg, Hessen und Rheinland-Pfalz haben die Angaben für ihre Ermittlungen verwendet. Der niedersächsische Landesverband des Hotels und Gaststätten Dehoga warf deshalb der Polizei eine Zweckentfremdung der Daten vor. Der Bundesbeauftragte für den Datenschutz Ulrich Kelber mahnte die Sicherheitsbehörden zur Zurückhaltung. Die Listen dürften nur bei „schwersten Straftaten" genutzt werden, nicht aber bei „kleineren Delikten oder Ordnungswidrigkeiten". Der rheinland-pfälzische Datenschutzbeauftragte Dieter Kugelmann forderte ein Bundesgesetz, das regelt, inwieweit die Polizei auf Corona-Gästelisten zurückgreifen darf. Dieses „Corona-Freiheitsschutz-Begleitgesetz" solle hohe Hürden für den Zugriff der Polizei vorsehen: „Wer im Biergarten sitzt, darf nicht später von der Polizei aufgrund des Eintrags in einer Corona-Gästeliste befragt werden, wenn es um die Aufklärung einer Ordnungswidrigkeit, einer kleineren Sachbeschädigung oder eines Falschparkens in der Nähe geht. Dies könnte unverhältnismäßig sein."

Gastronomiebetriebe forderte Kelber zur „datenschutzkonformen Ausgestaltung" der Kontaktlisten auf. Wenn offene Listen auslägen, müsse man sich nicht über falsche Angaben und Fantasienamen wundern. Ein Brauhaus im bayerischen Andechs vergibt an jeden Gast ein Formular, das von einem Mitarbeiter kontrolliert und dann in eine Box geworfen wird. Die Datenblätter kommen am Tagesende in einen Sicherheitsbeutel, der dann für vier Wochen im Tresor aufbewahrt und danach geschreddert wird. Einfacher erscheinen digitale Lösungen, etwa eine Registrierung der Kunden über einen QR-Code. Entsprechende Apps gibt es. Aber keine davon genügte bisher den Datenschutzstandards und war gegen Hackerangriffe hinreichend gesichert (Stalmann, Ein Bier mit Micky Maus, Der Spiegel Nr. 33 v. 08.08.2020, 47; Gästelisten-Gesetz gefordert, SZ 05.08.2020, 6).

Bundesweit

Digitale Corona-Gästedaten unsicher

Mitglieder des Chaos Computer Clubs (CCC), der großen deutschen Hacker-Organisation, waren bei einem Restaurantbesuch misstrauisch geworden, nachdem sie Namen und Kontaktdaten digital hinterlegen mussten. Die Gesundheitsbehörden wollen anhand dieser Daten Covid-19-Infektionsketten zurückverfolgen. Die Corona-Verordnungen verpflichten die Gastronomen, diese Daten zu erfassen. Bei ihren Recherchen fanden die Hacker dann tatsächlich schwere Sicherheitslücken in einer Cloud-Software, mit der 180 Restaurants Reservierungen und andere Daten verwalten. Der Fall wirft ein

schlechtes Licht auf den Datenschutz der Covid-19-Kontakterfassung. Die Cloud ist von überall aus zugänglich und wird vom Unternehmen Gastronovi aus Bremen angeboten. Nach eigenen Angaben verarbeiten seine Systeme jeden Monat im Schnitt 600.000 Reservierungen. In der Covid-19-Pandemie wirbt das Unternehmen damit, die eigene Software könne „die Daten Ihrer Gäste 100% datenschutzkonform“ speichern.

Über die Benutzerschnittstelle konnten sich die Hacker einfach Zugriff auf die Daten verschaffen. Wer im System sei, könne auch auf die Daten aller anderen Restaurants zugreifen, heißt es in einer Mitteilung des CCC, der 87.000 Corona-Kontakterhebungen fand. Auch Passwörter ließen sich demnach unbefugt auslesen, einige sogar im Klartext: „Triviale Passwörter wie 1234 deuteten auf das Fehlen einer angemessenen Passwortrichtlinie hin“. Der CCC geht davon aus, dass Gastronovi nur eines von vielen Unternehmen ist, die Passwörter ungenügend schützen. Wie es sich für ethisch saubere Hacker gehört, informierte der CCC zuerst das Unternehmen, bevor er den Fall öffentlich machte. Andreas Jonderko, Geschäftsführer Gastronovi Deutschland, erklärte, man habe „umgehend reagiert und die gefundenen Sicherheitslücken innerhalb weniger Stunden nach Erhalt des Berichts durch den CCC geschlossen“. Betroffene Gastronomen seien informiert worden. Johannes Caspar, Datenschutzbeauftragter des Landes Hamburg, äußerte sich zur Frage nach der Verantwortung: „Für die Einhaltung der Datenschutzvorschriften sind die Gaststättenbetriebe als Auftraggeber verantwortlich. Das betrifft auch die Löschung der Daten, soweit keine anderweitigen Vereinbarungen mit dem Auftragnehmer getroffen wurden.“

Die Kontaktdaten, die gegen die Verbreitung von Covid-19 helfen sollen, waren nicht die einzigen Infos, an die der CCC leicht herankam: „Im betroffenen System wurden jedoch nicht nur Corona-Listen, sondern auch Reservierungen, Bestellungen und Kassenumsätze gespeichert“ - insgesamt 4,8 Millionen Datensätze, vorwiegend aus Deutschland. Dem CCC zufolge reichen die Reservierungs-Daten sogar ein Jahrzehnt zurück. Covid-19-Kontaktdaten müssen nach vier Wochen gelöscht werden. Vor allem die lange Speicherung kritisierte der Bundesdatenschutzbeauftragte Ulrich Kelber: „Es ist inakzeptabel, dass nicht mehr benötigte Daten nicht gelöscht werden. Nicht jeder trifft sich einfach mal nur mit einem Kumpel.“ Whistleblower und Mandanten von Anwälten könnten so gefährdet werden.

Der CCC hat einen Tipp für Gäste, die mit digitalen Corona-Listen konfrontiert werden: Sie sollten eine E-Mail-Adresse einrichten, die sie ausschließlich für die Kontaktverfolgung nutzen. Gibt man seine Haupt-E-Mail-Adresse an, könnten Hacker oder Stalker sie missbrauchen. CCC-Sprecher Linus Neumann sagt: „Viele digitale Corona-Listen wurden mit der heißen Nadel gestrickt und machen schwer zu haltende Datenschutzversprechen. Die Sicherheit eines Papiersystems ist hingegen auch für Laien leicht zu beurteilen.“ Der CCC empfiehlt, jeder Besuchergruppe einen eigenen Zettel auszuhändigen. Die ausgefüllten Zettel eines Tages sollten dann jeweils in einem Umschlag sicher gelagert werden. Jeden Tag solle der Gastronom einen Umschlag vernichten, dessen Löschfrist abgelaufen sei. So machten die Hacker es auch in ihren eigenen „Hackspaces“, wo sie sich zum Tüfteln treffen (Brühl, Hauptgericht, Nachspeise, Datenleck, SZ 29./30.08.2020, 23).

Bundesweit

Office 365 nicht DSGVO-konform!?

Die Datenschutzaufsichtsbehörden in Deutschland streiten darüber, ob das Programmpaket Microsoft Office 365 regelkonform in Verwaltung und öffentlichen Einrichtungen eingesetzt werden kann. Eine Arbeitsgruppe der Datenschutzkonferenz (DSK), in der die Behörden von Bund und Ländern zusammenarbeiten, kam nach Sichtung von Verträgen und Unterlagen zu dem Schluss, dass „kein datenschutzgerechter Einsatz von MS Office 365 möglich“ ist. Vor allem die Bayerischen Landesdatenschützer stellten sich jedoch quer und trugen den Entwurf nicht mit. Die Formulierung sei „rechtlich fragwürdig“, schrieben sie in einer Rundmail von August 2020, in der sie ihre Ablehnung ankündigten. Der Beschluss würde die „naheliegende Frage nach konkreten Maßnahmen zur Aussetzung von MS 365 aufwerfen“. Auch sei man gegen eine Veröffentlichung des Papiers. Sollte die Mehrheit dies anders sehen, wünsche Bayern „eine ausdrückliche Kennzeichnung seiner Gegenstimme“. Die Deutschlandzentrale von Microsoft liegt in München. Schon im Herbst 2019 hatte eine Studie im Auftrag des Bundesinnenministeriums ergeben, dass 96% aller Bundesbehörden das MS-Office-Paket verwenden und „dringender Handlungsbedarf“ bestehe wegen der „starken Abhängigkeiten“ und „(datenschutz)rechtlicher Unsicherheiten“. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Ulrich Kelber bestätigte, es gebe zu dem Thema „weiteren Gesprächsbedarf“ sowohl intern als auch mit dem Microsoft-Konzern, mit dem die DSK „seit Längerem im Dialog“ sei. Ziel sei es, möglichst bald eine abschließende Bewertung abzugeben: „Dabei ist es mir wichtig, dass wir als Aufsichtsbehörden einheitlich agieren“ (Aufseher uneins über Microsoft, Der Spiegel Nr. 38 12.08.2020, 55).

Bundesweit

Bitkom-Umfrage zu DSGVO

Gemäß einer repräsentativen Bitkom-Befragung von 504 deutschen Unternehmen aller Branchen mit mehr als 20 Mitarbeitern gaben 56% der Firmen an, dass bei ihnen aufgrund der Datenschutz-Grundverordnung (DSGVO) „neue, innovative Projekte“ gescheitert seien. 41% sehen sich behindert, Datenpools aufzubauen, um etwa Daten mit Geschäftspartnern teilen zu können. Bei 31% der Unternehmen scheiterte angeblich an den EU-Vorgaben der Einsatz von Analyseverfahren wie Big Data oder Künstliche Intelligenz, ein knappes Viertel bestätigt dies für die Digitalisierung von Geschäftsprozessen.

Der Verband Bitkom stellte diese Ergebnisse auf seiner „Privacy Conference“ am 29.09.2020 vor. 92% der Umfrageteilnehmer fordern demnach, dass die DSGVO nachgebessert werden sollte, vor allem bei den Informationspflichten.

85% drängen darauf, die Regeln verständlicher zu machen. 83% wünschen sich eine bessere Beratung und mehr Hilfe von den Aufsichtsbehörden. Nur 3% meinen, dass die Verordnung verschärft werden sollte. 20% der Firmen haben die seit fast zweieinhalb Jahren anzuwendende DSGVO nach eigenen Angaben vollständig umgesetzt und einschlägige Prüfprozesse etabliert. 37% wollen die Regeln größtenteils implementiert haben, 35% teilweise. 6% haben mit dieser Arbeit gerade erst begonnen. Neun von zehn Unternehmen gehen davon aus, dass die Verordnung nicht komplett umsetzbar sei.

Die größte Herausforderung ist dabei für fast drei Viertel der Befragten eine ausgemachte Rechtsunsicherheit. 68% beklagen „zu viele Änderungen" oder Anpassungen bei der Auslegung des Normenwerks. 59% sehen als eines der größten Probleme die fehlenden Umsetzungshilfen durch Aufsichtsbehörden, 45% nennen die uneinheitliche Interpretation der Regeln innerhalb der EU. 26% beklagen einen Mangel an qualifizierten Mitarbeitern, während es im Vorjahr noch 37% waren. Mit Blick auf den eigenen Betrieb sieht die Mehrheit der Befragten die DSGVO kritisch. 71% monierten, dass die Verordnung ihre Geschäftsprozesse komplizierter macht, für 12% stellt sie eine Gefahr für etablierte Ansätze dar. Nur jedes fünfte Unternehmen erkennt für sich direkt mehr Vorteile. Sieben von zehn Firmen konstatieren aber allgemein, dass die DSGVO weltweit Maßstäbe für den Umgang mit personenbezogenen Daten setze, laut 66% führt sie zu einheitlicheren Wettbewerbsbedingungen. 62% sprechen von einem Wettbewerbsvorteil für die Wirtschaft in Europa.

Der Bitkom wollte auch wissen, wie sich Datenschutzvorgaben während der Corona-Krise auf die Betriebe auswirken: 26% nutzen demnach momentan Cloud-Dienste nur eingeschränkt oder nicht, insgesamt 40% bezogen dies auf Kollaborationswerkzeuge wie Microsoft Teams oder Slack für die Aufgabenkoordination und Kommunikation. Vier von zehn Firmen haben Homeoffice-Leitlinien, 22% haben diese erst mit der Pandemie eingeführt. Keine der Firmen hat eine eigene App zum Nachverfolgen von Corona-Infektionen entwickelt. Jedes fünfte Unternehmen ab 500 Mitarbeitern plant oder diskutiert aber den Einsatz einer eigenen Tracing-Anwendung unabhängig von der Corona-Warn-App (CWA) der Bundesregierung. 62% wünschen sich mehr Möglichkeiten, Daten nutzen zu können, um die Pandemie besser bekämpfen zu können.

Der Bundesdatenschutzbeauftragte Ulrich Kelber bezeichnete es als „spannend", dass fast 60% der Befragten meinten, den Umstellungsprozess geschafft zu haben. Zugleich verwies er neben tatsächlichen Problemen etwa beim Datentransfer auf eine „gefühlte Rechtsunsicherheit", die nicht ganz mit empirischen Fakten begründet sei. Rechtsanwälte und Berater hätten viele Firmen „auch zu Handlungen gebracht, die völlig überflüssig waren". Oft seien etwa riesige Prozesse, um die Einwilligung von Betroffenen einzuholen, nicht nötig und verhältnismäßig. Kelber widersprach der Klage über behinderte Innovation: „Es gibt Geschäftsmodelle, die wollen wir in Europa nicht", betonte er und zog eine Parallele etwa zur Kinderarbeit. Die Wirtschaft dürfe die informationelle Selbstbestimmung der Bürger nicht untergraben. Es reiche nicht, „den Datenschutz am Ende auf ein Projekt noch aufzupfropfen". Erfolgsversprechend sei es nur, wenn Entwickler Privacy by Design berücksichtigten.

Die DSGVO verständlicher zu machen, dürfte dem Bundesdatenschutzbeauftragten zufolge schwierig werden, da es sich um ein technologieneutrales, allgemein formuliertes Gesetz handeln müsse. Die Auslegungen müssten aber sehr konkret sein, weshalb etwa der Europäische Datenschutzausschuss schon viele Orientierungshilfen und Leitlinien herausgegeben habe. Mehr Beratungsbedarf gibt es laut Kelber vor allem bei den hiesigen Landesdatenschutzbehörden, von denen viele nach wie vor unterdimensioniert seien. Trotzdem seien auch hierzulande viele offizielle Hilfestellungen etwa für Homeoffice-Anwendungen verfügbar. Ein Rätsel sei ihm, warum in diesem Bereich bei vielen Werkzeuge von US-Anbietern „so omnipräsent in den Köpfen" seien. Vor allem bei Cloud- und Kollaborationsdiensten „existieren von deutschen Anbietern beste datenschutzkonforme Lösungen". Bei Pools müssten die Firmen zudem stärker unterscheiden etwa zwischen unproblematischen Maschinendaten und personenbezogenen Informationen (Krempl, Datenschutz-Korrekturen gefordert: Deutsche Firmen hadern mit der DSGVO, www.heise.de 29.09.2020, https://heise.de/-4915068).

Bundesweit

Auskunfteien planen Energieversorgungsvertragsdatei

Gemäß Medienrecherchen haben die Schufa und die Münchner Wirtschaftsauskunftei CRIF Bürgel Datenbanken entwickelt, in denen branchenweit Vertragsdaten möglichst vieler Kunden gespeichert werden sollen. Verbraucher- und Datenschützer fürchten, dass damit Energieversorger wechselfreudige Verbraucher identifizieren und in der Folge ablehnen könnten. Gemäß der Aussage von Barbara Saerbeck vom Bundesverband der Verbraucherzentralen (VZBV) sind Kunden, die schon nach der Mindestvertragslaufzeit wieder wechselten, für Energieversorger grundsätzlich unattraktiv und als „Bonushopper" verschrien. Wenn Strom- und Gasunternehmen durch solche Datenbanken künftig sehen könnten, dass Kunden schon häufiger gewechselt haben, könnten sie diese dann entweder systematisch ablehnen oder ihnen attraktive Konditionen vorenthalten.

Das Hamburger Portal „Wechselpilot" hat festgestellt, dass bei manchen Energieversorgern bereits jetzt jeder fünfte Neukunde abgelehnt wird. Häufig werden gemäß Geschäftsführer Jan Rabe für die Ablehnungen keine Gründe genannt. Abgelehnte Kunden müssten dann zu einem anderen Versorger und im ungünstigsten Fall in einen teuren Grundversorgungstarif.

Bisher dürfen Daten nur von Kunden, die ihre Rechnungen nicht zahlen oder die betrügen, branchenweit ausgetauscht werden. Man spricht von Negativdaten. Die neuen Datenbanken sollen dagegen auch Daten von vertragstreuen Kunden, sog. Positivdaten, enthalten. Der Datenschutzexperte und frühere Landesdatenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, kritisierte, dass solche Pools dazu führen, dass Verbraucher unter den Anbietern nicht mehr frei

wählen könnten. Die Kunden würden auf diese Weise „zum Freiwild der gesamten Branche“. Daher sei ein solches Auskunfteiangebot unzulässig.

Die größte deutsche Wirtschaftsauskunftei, die Schufa, konzipierte den Recherchen zufolge eine Datenbank namens „Schufa-E-Pool“. Darin sollen Energieversorger gemäß einem Werbeflyer „wertvolle Hinweise“ „durch Informationen zu dem bestehenden Energiekonto und der bisherigen Laufzeit“ finden. Die Unternehmen könnten diese Daten für ihren „Entscheidungsprozess im Neukundengeschäft“ einsetzen. Der „Schufa-E-Pool“ soll offenbar Antworten darauf liefern, wieviel Gas und Strom die Kunden verbrauchen und wie wechselfreudig sie sind.

Die Wirtschaftsauskunftei CRIF Bürgel entwickelte offenbar einen ähnlichen Pool für Energieversorger. Dessen Konzept wird gemäß den Medieninformationen von der zuständigen bayerischen Datenschutzbehörde geprüft. Das Unternehmen wollte sich auf Nachfrage nicht zu Details äußern. Ein Sprecher erklärte lediglich, dass man „generell keine Auskunft über mögliche zukünftige Projekte“ gebe. CRIF Bürgel wie auch die Schufa betonten, dass man sich stets an geltendes Recht halte. Schufa-Sprecher Ingo A. Koch erklärte, der „Schufa-E-Pool“ sei bislang nicht „marktfähig“: „Wir verfolgen die Idee grundsätzlich aber weiter.“ Es sei derzeit offen, „ob und wenn, in welcher Ausgestaltung“ sie wieder aufgegriffen werde. Die Datenbank wurde den Recherchen zufolge bis Mitte August 2020 im Internet sowie in einer aktuellen Unternehmensbroschüre beworben. Die Internetseite war erst entfernt worden, nachdem Medienvertreter zu den Hintergründen dieser Datenbank angefragt hatten. Bei der Vorstellung des „Schufa-E-Pools“ in einer Firmenbroschüre habe es sich um ein „redaktionelles Versehen“ gehandelt. Laut Schufa könnten Kunden, die sonst Schwierigkeiten beim Wechsel hätten, von der Datenbank profitieren.

Koch erklärte, „die Idee hinter dem E-Pool (sei) nicht das Verhindern eines Wechsels“. Entsprechenden Begehrlichkeiten aus der Energiewirtschaft sei die Auskunftei schon frühzeitig entgegengetreten. Es werde in der Datenbank „nach gegenwärtigem Entwicklungsstand lediglich die faktische und zeitliche Existenz des aktuellen Energiekontos gespeichert“ sowie gegebenenfalls unbezahlte Rechnungen. Mit solchen Informationen seien Energieversorger sogar in der Lage, Kunden als Vertragspartner anzunehmen, die sie sonst vielleicht nicht annehmen würden. Das sieht Verbraucherschützerin Barbara Saerbeck anders. Selbst wenn nur wenige Angaben zu Energiekonten gespeichert würden, bestehe die Gefahr, dass Kunden künftig diskriminiert würden. Die Angabe der Laufzeit reiche, um herauszufinden, ob jemand nach kurzer Zeit schon wieder wechseln wolle.

Die für Datenschutz zuständigen Aufsichtsbehörden der Bundesländer berieten in der ersten November-Woche 2020 darüber, ob sie solche Datenbanken für Energieversorger als zulässig ansehen. Der für die Schufa zuständige Hessische Landesbeauftragte für Datenschutz hält es aufgrund der Wettbewerbssituation für rechtlich vertretbar, dass Strom- und Gasversorger Kundendaten in branchenweiten Datenbanken teilten, so Michael Kaiser: „Wenn ich sehe, dass im Markt der Energieversorger schon die ein oder andere Insolvenz passiert ist – hauptsächlich aufgrund nutzloser Akquisitionskosten – dann muss ich dieses legitime Interesse einfach anerkennen.“ Vertreter anderer Datenschutzbehörden sehen eine solche Speicherung dagegen kritisch. Fünf Aufsichtsbehörden positionierten sich gegen den Datenpool: Der Landesdatenschutzbeauftragte von Mecklenburg-Vorpommern erklärte, er sehe keine Rechtsgrundlage dafür, alle Vertragsdaten der Strom- und Gaskunden zu speichern. Marit Hansen, seine Amtskollegin aus Schleswig-Holstein, konnte auch „nicht nachvollziehen“, weshalb solche Daten gespeichert werden sollen. Ähnlich ablehnend äußerten sich auch die Behörden von Hamburg, Rheinland-Pfalz und Baden-Württemberg. Von drei weiteren Behörden ist bekannt, dass sie entsprechende Vorbehalte gegen die geplanten Datenbanken haben.

Eine Medienumfrage unter 75 Strom- und Gasversorgern ergab ein uneinheitliches Bild. Zahlreiche Firmen berichteten, sie seien von den Auskunfteien wegen der Datenpools angesprochen worden. Einige erklärten, sie könnten sich eine Teilnahme vorstellen, sollten alle datenschutzrechtlichen Regelungen eingehalten werden, andere äußerten sich ablehnend. Eine Sprecherin des niedersächsischen Energieversorgers Firstcon meinte, der Wunsch nach einem „gläsernen Kunden“ sei zwar „aus wirtschaftlicher Perspektive nachvollziehbar, aber ethisch fragwürdig.“ Vattenfall ist an dem Projekt interessiert. Auch Konkurrent E.ON prüft die Pläne von Schufa und CRIF Bürgel.

Von den drei größten deutschen Energieversorgern mit Privatkundengeschäft äußerte sich nur EnBW klar ablehnend. E.ON dagegen räumte ein, „mit der Schufa und CRIF Bürgel im Rahmen von Projekten zusammengearbeitet und Datenpools geprüft“ zu haben. Über die Projektphase sei man aber nicht hinausgekommen. Vattenfall erklärte, man sei mit den beiden Auskunfteien „zu deren Produktportfolio im Austausch“. 25 Unternehmen, darunter Stromdiscounter wie Fuxx, Stromio und Immergrün beantworteten die Medienanfragen nicht.

Bundestagsabgeordnete sehen die Pläne der Auskunfteiunternehmen kritisch. Sebastian Steineke (CDU) sieht die Gefahr, dass einzelne Kunden diskriminiert werden. Reinhard Houben von der FDP betonte, dass Ablehnungen, nur weil jemand flexibel sein möchte, „nicht korrekt“ sein können. Tabea Rößner von den Grünen meinte, es könne nicht sein, dass „der Verbraucherschutz weiter ausgehebelt wird. Die Liberalisierung des Marktes solle doch den Verbrauchern die Möglichkeit geben, ihren Versorger frei zu wählen“. Und Ulla Jelpke von den Linken kommentierte: „Solchen Geschäftspraktiken muss ein Riegel vorgeschoben werden“ (Busch/Hornung, Mit der Schufa gegen „Bonushopper“, www.tagesschau.de 08.09.2020; Wischmeyer, Schwarze Liste für Bonus-Hopper, SZ 09.09.2020, 15; Wischmeyer, Behörden über Kritik an Datenpool, SZ 23.09.2020, 18).

Baden-Württemberg

Videovollüberwachung bei Müller Fleisch

Müller Fleisch ist einer der größten Schlacht- und Fleischzerlegungsbetriebe in Süddeutschland. Dieser überwacht

seit Jahren seine meist aus Osteuropa stammenden Mitarbeiter während der Produktion. Etwa 60 Kameras sind in „produktionsnahen Bereichen" installiert. Zwei Drittel befinden sich, so die Angaben des Unternehmens, in Randbereichen; hauptsächlich gehe es um die Überwachung der Anlagen. Die übrigen würden die Produktion „ins Visier" nehmen. Die Kameras seien zwar auf die technischen Abläufe fixiert, aber „gelegentlich" seien auch Mitarbeiter unverpixelt zu sehen. Wenn sie als Ganzes zu sehen sind, dann seien sie wegen der Hygienekleidung nicht zu identifizieren.

Angestellte berichten dagegen etwas ganz anderes: Die Aufnahmen zeigten eindeutig erkennbar die in der Herstellung tätigen Arbeiter. Dies lässt sich auch aus den Kamerapositionen erkennen. Die Kameras laufen ständig. Die Geschäftsleitung kann die Aufnahmen über Bildschirme in ihren Büros verfolgen. Dies führt nach Angaben der Angestellten dazu, dass etwa Martin Müller, Spross des Gründers, in der Produktion aufschlägt und vermeintliche Trödler ermahnt. Die Firma räumt ein, dass die Betriebsleitung die Aufnahmen einsieht, behauptet aber, dass sie diese nicht zur Maßregelung nutze. Müllers Visiten im Betrieb zeigten „die Nähe vom Inhaber zu seinen Mitarbeitern".

Stefan Brink, Datenschutzbeauftragter von Baden-Württemberg meint dagegen: „Wenn Mitarbeiter, wie es hier scheint, in erheblichem Umfang während der Arbeitszeit überwacht werden, ist das rechtswidrig." Ständig den Arbeitgeber im Nacken zu spüren sei ein Eingriff in die Persönlichkeitsrechte, den Arbeitsgerichte in jahrelanger Tradition immer wieder untersagt hätten. Die Zustimmung eines willfährigen Betriebsrats rechtfertige eine Bespitzelung ebenso wenig wie der vom Unternehmen angeführte Schutz vor Diebstahl, so Brink: „Viel zu allgemein". Und selbst wenn man nur Arme und Oberkörper sähe, wie Müller angibt, könne man durch Schichtpläne Rückschlüsse auf die einzelnen Personen ziehen.

Dass die Arbeitsatmosphäre bei Müller Fleisch zwischen Unternehmensleitung und Mitarbeitenden unterschiedlich bewertet wird, kann der Webseite des Konzerns, wo von sensibilisierter Leitkultur die Rede ist, und der Bewertungsplattform Kununu entnommen werden. Dort berichten Beschäftigte in Bezug auf Vorgesetztenverhalten „komplette Katastrophe", Kommunikation „nicht vorhanden" und Arbeitsbedingungen „wie im Mittelalter". Eine Personalreferentin bemühte sich um Schadenbegrenzung, als sie mitteilte, man habe die Verbesserungsvorschläge zur Kenntnis genommen und „durchleuchte" diese.

Immer wieder fällt die Fleischbranche unangenehm in Bezug auf das Mitarbeiterüberwachen auf. Ihre osteuropäische Arbeitstrupps sind kaum in der Lage, sich hiergegen zu wehren. Die Tönnies-Gruppe musste im Jahr 2010 80.000 € Bußgeld zahlen; Kameras filmten dort sogar in Damenumkleiden. Müller Fleisch erklärte zu den Vorwürfen, die eigenen Kameras seien gesetzeskonform; dazu gebe es eine Betriebsvereinbarung. Die Kameras verfügen gemäß Herstellerangaben über einen sehr guten Zoom und eine ausgezeichnete Panoramasicht (Klawitter, Gläserne Produktion, Der Spiegel Nr. 39 19.09.2020, 67).

Baden-Württemberg

Erneute Novelle des Polizeirechts geplant

Nachdem erst Ende 2017 das Polizeigesetz des Landes Baden-Württemberg novelliert worden ist, plant Innenminister Thomas Strobl (CDU) schon die nächste Novelle. Im Innenausschuss des Landtags wurde im Juli 2020 der ins Stocken geratene Zeitplan dafür abgestimmt. Im November 2017 hatte das von Strobl eingebrachte Gesetz Verschärfungen gebracht; die Polizei erhielt etliche neue Kompetenzen. Die Reform stand unter dem Eindruck dschihadistischer Terroranschläge. Es ging unter anderem um die digitale Überwachung von Verdächtigen, Fußfesseln für Gefährder oder die Ausrüstung von Spezialeinheiten mit Handgranaten (DANA 4/2017, 210).

Bei der nun vorgesehenen zweiten Reform in dieser Legislaturperiode soll zum einen das Gesetz an die EU-Richtlinie zum Datenschutz für Justiz und Inneres angepasst werden. Die Richtlinie aus dem Jahr 2016 hätte bis zum Mai 2018 umgesetzt werden müssen. Außerdem erfordern zwei Entscheidungen des Bundesverfassungsgerichts Änderungen: ein Urteil von 2016 zum Bundeskriminalamtsgesetz und ein Beschluss von 2018 zum Einsatz automatischer Kennzeichenlesesysteme. Darüber hinaus will Strobl der Polizei erneut mehr Befugnisse einräumen.

Auf dem Beteiligungsportal der Landesregierung steht eine Version eines Entwurfes, der aber noch im Innenministerium weiter bearbeitet wird. Geht man danach, so wird sehr viel überarbeitet. Allein die Änderungen des Gesetzes umfassen 150 A4-Seiten, dazu kommen 124 Seiten Begründung. Doch nicht jede Änderung steht für eine neue Rechtsgrundlage. Das Gesetz soll generalüberholt und neu durchstrukturiert werden.

Vor allem zwei inhaltliche Punkte aus Strobls anfangs sehr umfangreichem Forderungskatalog haben die monatelangen Verhandlungen mit seinem Koalitionspartner, den Grünen, überstanden und sollen eingeführt werden: Der Einsatz sogenannter Bodycams, von Polizisten am Körper getragener Kameras, soll ausgeweitet werden. Außerdem sollen Kontrollen und Durchsuchungen von Personen im Rahmen öffentlicher Veranstaltungen erleichtert werden. Bodycams sollen auch in geschlossenen Räumen benutzt werden dürfen, nicht mehr nur im Freien. Der polizeipolitische Sprecher der CDU-Fraktion, Siegfried Lorek, erklärte dazu im Landtag mit Blick auf Jugendkrawalle in Stuttgart: „Stellen Sie sich mal den Fall vor, ein Polizist wäre da einem Plünderer hinterhergelaufen und hätte durch eine Schaufensterscheibe einen Laden betreten. Dann hätte der Polizist an der Schaufensterscheibe die Bodycam ausschalten müssen. Das ist völlig absurd." Der SPD-Innenpolitiker Sascha Binder fürchtet, durch die Reform werde die Rechtslage noch komplizierter. Er fordert, Polizisten besser für die bisher zulässige Nutzung zu schulen.

Das polizeiliche Recht für Personenfeststellungen und Durchsuchungen soll erweitert werden. So sollen Beamte ohne Anlass eine Person durchsuchen dürfen, wenn diese „bei oder im Zusammenhang mit öffentlichen

Veranstaltungen und Ansammlungen angetroffen wird, die ein besonderes Gefährdungsrisiko (...) aufweisen und dort erfahrungsgemäß mit der Begehung von Straftaten gegen Leib, Leben oder Sachen von bedeutendem Wert zu rechnen ist".

Kritiker halten die Regelungen für zu weitgehend. Der innenpolitische Sprecher der FDP-Fraktion, Ulrich Goll, sagte: „Identitätsfeststellungen oder gar Durchsuchungen stellen für die Betroffenen einen erheblichen Freiheitseingriff dar. Die Voraussetzungen dafür müssen sich eindeutig aus dem Gesetz ergeben. Der bloße Verweis auf polizeiliche Erfahrungswerte ist zu unbestimmt und muss nachgebessert werden." Der Deutsche Anwaltsverband hat ein Gutachten erstellt, in dem er darlegt, dass das neue Gesetz aus vielfältigen Gründen gegen das Grundgesetz verstoßen würde. Manche Bürgerrechtsorganisationen gehen in ihrer Kritik noch weiter. Polizeigewerkschaften dagegen unterstützen das Reformvorhaben (Habermehl, Die nächste Polizeireform, www.tagblatt.de 07.07.2020).

Baden-Württemberg

Tübingens OB Palmer will Straftäterdaten von Asylbewerbern

Tübingens Oberbürgermeister Boris Palmer (Grüne) forderte in einem Brief an Bundesinnenminister Horst Seehofer (CSU) eine Regelung, die einen Datenaustausch zwischen Polizei und Kommunen „für effektive Kriminalprävention und Integration" ermöglicht: „Der Staat darf sich nicht so weit selbst beschränken, dass die rechte Hand nicht mehr weiß, was die linke tut." Hintergrund ist ein Streit um den Datenschutz. In Tübingen hatte Palmer einen „strukturierten Informationsaustausch" etabliert, in dem neben der Ausländerbehörde auch die Abteilung „Hilfe für Geflüchtete" Zugriff auf eine von der Stadt geführte Liste mit straffälligen und gewaltbereiten Asylbewerbern hatte. Diese Praxis wurde vom Landesbeauftragten für Datenschutz Stefan Brink untersagt: Ermittlungsdaten der Polizei unterlägen einer strengen Zweckbindung und dürften nicht pauschal für andere Zwecke genutzt werden.

Diese enge Auslegung hält Palmer für falsch. „Eine Gesellschaft muss auch fordern, damit Integration gelingt", schreibt er an Seehofer. Vor allem die kleine Gruppe der Mehrfachstraftäter unter den Asylbewerbern sei für einen großen Teil der Probleme verantwortlich. Das sei „kein Pauschalurteil": 95% der Asylbewerber verhielten sich friedlich. Bei Personen, die „verstärkte Gewaltbereitschaft" erkennen ließen, müsse man aber auch als Kommune gegensteuern können – etwa durch Sozialarbeit: „Es ist auch im Sinne der Geflüchteten richtig und notwendig, frühzeitig zu intervenieren, bevor sie auf die schiefe Bahn geraten."

Derzeit sei eine enge Zusammenarbeit zwischen Polizei und Sozialbehörden nicht möglich, da Informationen über Straftaten nur an die Ausländerbehörde, nicht aber an Sozialarbeiter fließen dürften. Durch die Beschränkung könne bei Geflüchteten der Eindruck entstehen, „dass selbst tätliche Angriffe mit einem Messer in Deutschland keinerlei Konsequenzen haben". Auch zum Schutz der Mitarbeiter seien solche Informationen wichtig, um tätliche Übergriffe zu vermeiden: Beratungsgespräche mit Personen von der besagten „Liste auffälliger Asylbewerber" seien zuletzt in Tübingen stets mit zwei Beschäftigten durchgeführt worden. Palmer fordert eine Erweiterung der Daten-Zweckbindung, die in Form einer Verordnung oder „nötigenfalls" per Gesetz regelt, „dass Sicherheitsbehörden, Ausländerbehörde und Sozialbehörde sinnvoll zusammenarbeiten können. Das dient der Gefahrenabwehr wie der Integration gleichermaßen" (Müller, Asylbewerber-Liste: Palmer bittet Seehofer um Hilfe, www.tagblatt.de 20.10.2020).

Bayern

Schüler mit Anti-Masken-Attest isoliert

Sechs Kinder an einer Realschule in Roding im Kreis Cham wurden von ihren eigentlichen Klassen getrennt, weil sie per ärztlichem Attest von der Maskenpflicht befreit sein sollten. Der Schulleiter Alexander Peintinger begründete seine Maßnahme mit der Zunahme solcher Atteste: „Die Eltern reden mit mir nicht darüber, was dem Kind fehlt, das bin ich anders gewohnt." Die Eltern hätten das Attest nicht einmal aus der Hand gegeben; der Schulleiter durfte es nicht kopieren und nur im Stehen durchlesen. Besonders suspekt war für ihn, dass die Atteste zeitlich unbegrenzt und alle von derselben Praxis im Nachbarlandkreis Schwandorf kamen. Deshalb hatte der Schulleiter „erhebliche Zweifel" und reichte eine Beschwerde bei der Bayerischen Landesärztekammer ein. Diese nahm die Beschwerde an und prüft sie. Peintinger erklärte: „Ich hätte den Schülern den Zugang zur Schule eigentlich verweigern müssen. Es gilt nun einmal Maskenpflicht. Ich habe eine Verantwortung allen Schülern gegenüber." Das habe er mit seiner beruflichen Einstellung jedoch nicht vereinbaren können, weshalb er die Schüler in einem separaten Klassenzimmer betreuen ließ. Bisher gab es an der Schule keinen Corona-Fall, das solle auch so bleiben. Das Verwaltungsgericht Würzburg sowie der Bayerische Verwaltungsgerichtshof hatten derweil Eilanträge gegen die Maskenpflicht für Grundschüler abgewiesen. Eltern hatten Atteste vorgelegt, in denen es ohne weitere Begründung hieß, sie könnten „aus gesundheitlichen Gründen" die Masken nicht tragen (Masken-Atteste lösen Verwirrung aus, SZ 28.10.2020, 22).

Bayern

Diözesandatenschutzbeauftragter beklagte fehlende Ressourcen

Der Diözesandatenschutzbeauftragte für die bayerischen Diözesen, Jupp Joachimski, sieht aufgrund zu geringer personeller und finanzieller Ausstattung seine Behörde auf Dauer nicht in der Lage, die rechtlichen Mindestanforderungen für eine kirchliche Datenschutzaufsicht zu erfüllen. In seinem am 12.10.2020 veröffentlichten Tätigkeitsbericht beklagt er, dass „die bayerische kirchliche Datenschutzaufsicht stark hinter den vergleichbaren Dienststellen anderer Bundesländer,

aber auch gegenüber staatlichen Datenschutzaufsichten" zurückbleibe und auf Dauer so die rechtlich geforderte Gleichwertigkeit der kirchlichen Datenschutzaufsicht mit den staatlichen Behörden in Frage stehe. Zudem sei eine Mitarbeit in den bundesweiten Gremien der kirchlichen Datenschutzaufsichten kaum möglich. Er berichtet von einem seit Inkrafttreten des Gesetzes über den kirchlichen Datenschutz (KDG) im Mai 2018 um 300% gestiegenen Aufkommen an Beschwerden von Betroffenen über Datenschutzverletzungen. Die Anzahl der Anzeigen von Datenpannen habe sich seither von ein bis zwei Meldungen pro Jahr auf zwei bis drei pro Woche erhöht. Im Bericht geht er außerdem auf Details zu den Beschwerden und Datenschutzverletzungen ein.

Joachimski, der das Amt des Diözesandatenschutzbeauftragten in Teilzeit ausfüllt, stehen zwei Planstellen zur Verfügung, von der eine seit 2018 nicht besetzt werden konnte. Die Aufsichtstätigkeit kann aufgrund des Fehlens eines Vertreters laut Bericht nur dadurch sichergestellt werden, dass der Diözesandatenschutzbeauftragte auch während des Urlaubs weiterarbeitet. Auch die Büroorganisation obliegt vollständig dem Behördenleiter. Die für einen ähnlich großen Bereich zuständige nordrhein-westfälische Aufsichtsbehörde, das Katholische Datenschutzzentrum Dortmund, kann laut dessen Tätigkeitsbericht über elf Planstellen verfügen.

Für die bayerische Aufsicht sieht Joachimski sechs Planstellen als ausreichend an. Die gegenwärtige Ausstattung lasse sich aber aufgrund der besonderen Situation im Hinblick auf den geplanten Umzug nach Nürnberg „zeitweise" vertreten. Das in Bayern praktizierte System „Leitender betrieblicher Datenschutzbeauftragter" in den einzelnen Diözesen, die für das Datenschutzmanagement zuständig sind, entlaste zudem die Aufsicht.

2018 hatte die Freisinger Bischofskonferenz die Einrichtung eines kirchlichen Datenschutzzentrums in Nürnberg beschlossen, die allerdings noch nicht umgesetzt wurde. Laut Bericht wurde die Anerkennung als Körperschaft des öffentlichen Rechts beantragt, ein Zeitplan ist dem derzeitigen Chef der Aufsichtsbehörde jedoch nicht bekannt. Die Amtszeit des ehemaligen Vorsitzenden Richters am bayerischen Obersten Landesgerichts als Diözesandatenschutzbeauftragter sollte Ende September 2020 enden. Bis zur Benennung eines Nachfolgers führt er das Amt kommissarisch weiter.

Die seit Mai 2018 geltende EU-Datenschutzgrundverordnung erlaubt es Kirchen und Religionsgemeinschaften, unter bestimmten Bedingungen eigenes Datenschutzrecht anzuwenden und kirchliche Datenschutzaufsichten einzurichten, die die Einhaltung der kirchlichen Gesetze überwachen. Dabei muss allerdings sichergestellt sein, dass innerhalb der Religionsgemeinschaften ein Datenschutzniveau herrscht, das im Einklang mit dem EU-Recht steht. In Deutschland haben die katholische und die evangelische Kirche sowie mehrere kleinere Religionsgemeinschaften von der Klausel Gebrauch gemacht und wenden eigenes Datenschutzrecht an. In Deutschland gibt es fünf katholische Datenschutzaufsichten in Bremen, Dortmund, Frankfurt am Main, München und Schönebeck, die jeweils für mehrere Bistümer zuständig sind (Bayerische kirchliche Datenschutzaufsicht kann Aufgaben kaum erfüllen, www.katholisch.de 12.10.2020).

Hamburg/Bayern

Sensitive Beschäftigtendatensammlung bei H&M

Im Fall der Überwachung von mehreren hundert Mitarbeiterinnen und Mitarbeitern des H&M Callcenters in Nürnberg durch die Center-Leitung hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) einen Bußgeldbescheid in Höhe von 35.258.707,95 Euro gegen die H&M Hennes & Mauritz Online Shop A.B. & Co. KG erlassen, die ihren Sitz in Hamburg hat. Mindestens seit dem Jahr 2014 kam es bei einem Teil der Beschäftigten zu umfangreichen Erfassungen privater Lebensumstände. Entsprechende Notizen wurden auf einem Netzlaufwerk dauerhaft gespeichert. Nach Urlaubs- und Krankheitsabwesenheiten – auch kurzer Art – führten die vorgesetzten Teamleader einen sog. Welcome Back Talk durch. Nach diesen Gesprächen wurden in etlichen Fällen nicht nur konkrete Urlaubserlebnisse der Beschäftigten festgehalten, sondern auch Krankheitssymptome und Diagnosen, „von der Blasenschwäche bis zur Krebserkrankung", so der HmbBfDI Johannes Caspar. Einige Vorgesetzte eigneten sich über Einzel- und Flurgespräche ein breites Wissen über das Privatleben ihrer Mitarbeitenden an, das von eher harmlosen Details bis zu familiären Problemen sowie religiösen Bekenntnissen reichte. Die Erkenntnisse wurden teilweise aufgezeichnet, digital gespeichert und waren mitunter für bis zu 50 weitere Führungskräfte im ganzen Haus lesbar. Die Aufzeichnungen wurden bisweilen mit einem hohen Detailgrad vorgenommen und im zeitlichen Verlauf fortgeschrieben. Die so erhobenen Daten wurden neben einer akribischen Auswertung der individuellen Arbeitsleistung u.a. genutzt, um ein Profil der Beschäftigten für Maßnahmen und Entscheidungen im Arbeitsverhältnis zu erhalten. Die Kombination aus der Ausforschung des Privatlebens und der laufenden Erfassung, welcher Tätigkeit sie jeweils nachgingen, führte zu einem besonders intensiven Eingriff in die Rechte der Betroffenen.

Bekannt wurde die Datenerhebung dadurch, dass die Notizen infolge eines Konfigurationsfehlers im Oktober 2019 für einige Stunden unternehmensweit zugreifbar waren. Nachdem der HmbBfDI über die Datensammlung durch Presseberichte informiert worden war, ordnete er zunächst an, den Inhalt des Netzlaufwerks vollständig „einzufrieren" und verlangte dann die Herausgabe. Das Unternehmen kam dem nach und legte einen Datensatz von rund 60 Gigabyte zur Auswertung vor. Vernehmungen zahlreicher Zeuginnen und Zeugen bestätigten nach Analyse der Daten die dokumentierten Praktiken.

Die Verantwortlichen sahen sich zur Ergreifung verschiedener Abhilfemaßnahmen veranlasst. Dem HmbBfDI wurde ein umfassendes Konzept vorgelegt, wie künftig am Standort Nürnberg Datenschutz umgesetzt werden soll. Zur Aufarbeitung der vergangenen Geschehnisse hat sich die Unternehmensleitung nicht nur ausdrücklich bei den Betroffenen entschuldigt. Sie folgt

auch der Anregung, den Beschäftigten einen unbürokratischen Schadenersatz in beachtlicher Höhe auszuzahlen. Es handelt sich, so der HmbBfDI, insoweit um ein bislang beispielloses Bekenntnis zur Unternehmensverantwortung nach einem Datenschutzverstoß. Weitere Bausteine des neu eingeführten Datenschutzkonzepts sind unter anderem ein neu berufener Datenschutzkoordinator, monatliche Datenschutz-Status-Updates, ein verstärkt kommunizierter Whistleblower-Schutz sowie ein konsistentes Auskunfts-Konzept. Nach dem Vorgang wurde in Nürnberg ein Betriebsrat eingerichtet.

Caspar erklärte zum Bußgeld, dieses sei „in seiner Höhe angemessen und geeignet, Unternehmen von Verletzungen der Privatsphäre ihrer Beschäftigten abzuschrecken". Das Bemühen der Konzernleitung sei positiv zu bewerten, die Betroffenen vor Ort zu entschädigen und das Vertrauen in das Unternehmen als Arbeitgeber wiederherzustellen. H&M hatte für den Sachverhalt den BigBrotherAward 2020 im Bereich Arbeitswelt erhalten (HmbBfDI, PE 01.10.2020, 35,3 Millionen Euro Bußgeld wegen Datenschutzverstößen im Servicecenter von H&M; https://bigbrotherawards.de/2020/arbeitswelt-hm-hennes-und-mauritz).

Nordrhein-Westfalen

Bosbach-Kommission fordert zusätzliche Kompetenzen für Sicherheitsbehörden

Der Ministerpräsident von Nordrhein-Westfalen Armin Laschet, der sich um den CDU-Bundesvorsitz und die Kanzlerkandidatur seiner Partei bewirbt, will den Bericht einer Expertenkommission zur Inneren Sicherheit nutzen, um für Gesetzesverschärfungen auf Bundesebene zu werben: Deutschland brauche „auch im Bund eine grundsätzliche Inventur der Sicherheits-Architektur". Laschet stellte in Düsseldorf den 150 Seiten starken Bericht der drei Jahre zuvor eingesetzten Kommission unter Vorsitz seines Parteifreundes Wolfgang Bosbach vor.

Diese sogenannte Bosbach-Kommission empfiehlt die Überwachung islamistisch radikalisierter Kinder unter 14 Jahren durch den Verfassungsschutz oder auch eine Obergrenze für Barzahlungen beim Kauf von Immobilien oder teuren Autos zur Bekämpfung der Geldwäsche. Bosbach erläuterte: „Deutschland gilt hier als El Dorado". Politisch umstritten ist der Vorschlag der Kommission, Verfassungsschutzbehörden den Zugriff auf verschlüsselte Messenger-Dienste wie WhatsApp zur Überwachung „relevanter Personen" zu erlauben. Der frühere Bundesinnenminister Gerhart Baum (FDP) wies darauf hin, dass hier „eine sehr sensible Zone" bürgerlicher Freiheit berührt werde und eine Überwachungsbefugnis für den Verfassungsschutz „weitaus vorsichtiger gestaltet werden (müsse) als etwa bei der Polizei", da letztere strengeren richterlichen Kontrollen unterliege.

Laschet selbst machte sich drei andere Vorschläge der insgesamt 15 Experten zu eigen. Er unterstützte die Idee, durch die Veröffentlichung von Fotos mutmaßlicher Straftäter schneller und häufiger als bisher die Bevölkerung bei Fahndungen einzubinden. Zudem will Laschet eine präzisere und gerichtsverwertbare Ortung des Handys eines Tätern zur Tatzeit erreichen, indem die exakte Größe und Stärke der Funkzellendaten bei den Mobilfunkbetreibern ermittelt und kartographiert werden. Bisher erheben nur Bayern und Baden-Württemberg diese Daten. Zuletzt griff Laschet den Vorschlag auf, nach dem Vorbild von Fingerabdrücken oder DNS-Spuren künftig auch die Abgleiche von Ohr-Abdrücken und von Schuhsohlen-Abdrücken zentral zu speichern. Solche „automatisierte Datenbanken zum Spurenabgleich" können nach Meinung der Kommission vor allem die Fahndung nach Einbrechern unterstützen (Wernicke, Fotos und Ohr-Abdrücke, SZ 07.08.2020, 5).

Schleswig-Holstein

Marit Hansen als ULD-Chefin bestätigt

Der bisherigen Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und Landesdatenschutzbeauftragten wurde am 28.09.2020 vom Ministerpräsident des Landes Daniel Günther die Ernennungsurkunde für ihre zweite Amtszeit übergeben. Am 18.06.2020 war sie einstimmig vom Schleswig-Holsteinischen Landtag wiedergewählt worden. Die lange Dauer zwischen Wahl und Ernennung erklärt sich damit, dass zunächst das von einem Mitbewerber angerufene Schleswig-Holsteinische Verwaltungsgericht das Verfahren überprüfen musste (DANA 3/2020, 191 ff.). Das Gericht sah jedoch keinen Grund zur Beanstandung, die Landesregelungen seien konform mit den europarechtlichen Anforderungen.

Hansen freute sich und wies darauf hin, dass die Ernennung auf einen besonderen Tag fiel: den „Right To Know Day", den Internationalen Tag der Informationsfreiheit: „Meine Dienststelle und ich sind nicht nur für Datenschutz zuständig, sondern auch für den Zugang zu Informationen bei öffentlichen Stellen. In Sachen Transparenz ist das Land Schleswig-Holstein schon auf einem guten Weg, aber die Behörden können noch besser werden." Hansen spricht sich nicht nur für „Datenschutz by Design" aus, sondern sieht auch ein großes Potential in der „Informationsfreiheit by Design" (ULD, PM 28.09.2020, Zweite Amtszeit für die Landesbeauftragte für Datenschutz Marit Hansen).

Schleswig-Holstein

Kritik der Politik an ULD-Ermittlungen nach Dokumenten-Leak

Datenschutzrechtliche Ermittlungen des Unabhängigen Landeszentrums für Datenschutz (ULD) sorgten im Landtag Schleswig-Holstein für hitzige Diskussionen: Der Norddeutsche Rundfunk (NDR) hatte im Mai 2020 über eine Dienstaufsichtsbeschwerde gegen die Polizeibeauftragte des Landes, Samiah El Samadoni, berichtet, die ihm zuvor zugespielt worden war. Diese schaltete daraufhin die Datenschutzbeauftragte des Landes, Marit Hansen, ein. Deren Behörde, das ULD, untersuchte das Filmmaterial des NDR, um Hinweise auf das mögliche Datenleck zu finden. Dabei stellte das ULD fest, dass die Herkunft des im Fernsehen abgebildeten Dokuments auf Grund bestimmter Eigenschaften eingegrenzt und dass ein

Datenleak beim Ältestenrat des Landtags nicht ausgeschlossen werden kann.

Dies stieß auf Kritik des schleswig-holsteinischen Bundestagsabgeordneten und FDP-Bundesvize Wolfgang Kubicki: Aufgabe sei es nur, Verstöße gegen den Datenschutz aufzudecken, nicht Quellen von Journalisten. Er sieht hierin eine Grenzüberschreitung und Gefahr: „Denn das würde dazu führen, dass alle Whistleblower, diejenigen, die etwas weitergeben, wenn sie glauben, es läuft etwas falsch im Staate, durch den Datenschutz kriminalisiert werden, was sicher nicht sein kann." SPD-Fraktionschef Ralf Stegner dagegen meinte, die Pressearbeit sei nicht betroffen, „weil es ja nicht darum geht, dass irgendjemandem etwas vorgeworfen wird, der das Dokument bekommen und verwendet hat." Das sei in der Tat Pressefreiheit. Aber, so Stegner weiter: „Der das übermittelt hat, der hat ziemlich sicher gegen Recht verstoßen. Das ist ein schwerwiegender Vorgang."

Hansen wies Vorwürfe gegen ihre Behörde in diesem Zusammenhang zurück: „Wenn es sich um Datenschutzverstöße handelt, personenbezogene Daten, die so nicht weitergegeben werden dürfen, wo auch welche geschädigt werden können durch Berichterstattung, dann haben die Betroffenen das Recht uns anzurufen." Die Aufgaben ihrer Behörde seien klar definiert, auch die Grenzen der Befugnisse. So könne das ULD, anders als möglicherweise die Staatsanwaltschaft, beim NDR keine Razzia durchführen. Im Fall der weitergereichten Dienstaufsichtsbeschwerde hat das ULD das Verfahren eingestellt. Es konnte, so Hansen, nicht herausgefunden werden, von wem das Dokument weitergegeben wurde. Die Staatsanwaltschaft ermittelt weiter (Böhnke, Fall El Samadoni: Dürfen Datenschützer nach Quellen suchen? www.ndr.de 24.09.2020).

Datenschutznachrichten aus dem Ausland

Weltweit

Corona beschleunigt Überwachung

Freedom House

Ein Bericht der nichtstaatlichen US-Bürgerrechtsorganisation „Freedom House" beschreibt, wie die Corona-Pandemie in vielen Ländern missbraucht wird, um neue Instrumente zur digitalen Überwachung zu schaffen. Die Pandemie habe zu einem „dramatischen Verfall" der Freiheit im Internet geführt. In ihrem jährlichen „Freedom on the Net Report" untersucht die Organisation, wie es international um die digitale Redefreiheit und das Recht auf die eigenen Daten steht. 2020 zeigt sich danach ein „besonders düsteres" Bild: Staatliche und private Akteure in zahlreichen Ländern hätten die Krise genutzt, um online veröffentlichte Informationen zu steuern, kritische Berichte zu unterdrücken und neue Technologien zur sozialen Kontrolle zu installieren.

Der Bericht beschreibt, wie in einer Pandemie ein freier Zugang zu Informationen „den Unterschied zwischen Leben und Tod bedeuten" kann. Behörden in mindestens 28 von 65 untersuchten Ländern haben danach Websites gesperrt oder einzelne Nutzer, Plattformen oder Online-Publikationen gezwungen, Informationen über die Ausbreitung der Pandemie zu löschen. In mindestens 13 Ländern sei das Internet zeitweise ganz abgeschaltet worden, besonders häufig in Regionen, in denen Minderheiten leben. Neue Gesetze zur Eindämmung vermeintlich falscher Nachrichten über das Infektionsgeschehen oder zum Erhalt der öffentlichen Ordnung würden vielfach missbraucht. Zu beobachten sei das innerhalb der EU etwa in Ungarn gewesen, wo ein Mann, der Premierminister Viktor Orbán auf Facebook wegen dessen Corona-Politik einen „grausamen Tyrannen" genannt hat, wegen „Panikmache" inhaftiert worden ist.

Der Bericht widmet sich ausführlich den Corona-Apps, die in zahlreichen Ländern im Einsatz sind, um Träger des Virus zu identifizieren und deren Kontakte nachzuvollziehen. Es ist möglich, diese Apps so zu programmieren wie die deutsche Corona-Warn-App, wo Informationen nicht zentral gespeichert, sondern lediglich mit einem Pseudonym versehen direkt zwischen den Nutzern ausgetauscht werden. In mindestens 54 Ländern aber existieren laut dem Bericht nur minimale Vorkehrungen gegen den Missbrauch solcher sensiblen Informationen, die zudem vielfach mit bereits existierenden, öffentlich oder privatwirtschaftlich erhobenen Daten über die Bürger gekoppelt und an verschiedene Behörden weitergegeben werden. Die russische App zur Kontaktverfolgung teile etwa GPS-Daten, Anruflisten und andere Informationen mit dem wachsenden russischen Überwachungsapparat. Zudem verlangt sie unter Strafandrohung in unregelmäßigen Abständen Selfies der Nutzer, die damit beweisen sollen, dass sie sich an Quarantäne-Verordnungen halten. Ähnlich in Indien, wo unter Beamten im Scherz gesagt werde: „A selfie an hour keeps the police away".

In mindestens 30 Ländern finden laut dem Bericht Überwachungsmaßnahmen in direkter Partnerschaft mit Telekommunikationsanbietern und anderen Unternehmen statt. Die händigten den Regierungen die Kontaktdaten der Bürger aus. Besonders besorgniserregend sei, dass mit der Verarbeitung solcher Daten in vielen Fällen nationale Sicherheits- und Militärbehörden betraut werden, etwa in Pakistan, wo der Geheimdienst der Streitkräfte, dem Menschenrechtsverletzungen vorgeworfen werden, nun Kontaktnachverfolgung betreibe. In pakistanischen Geheimdienstberichten sei die Rede von abgehörten Telefonaten in Krankenhäusern, mit denen ermittelt werden solle, ob Freunde und Bekannte von Patienten ebenfalls Symptome zeigen.

Südkoreanische Beamte griffen auf Kreditkartenabrechnungen, Handystandorte und Sicherheitskameras zu, um die Ausbreitung des Virus zu überwachen. Der Bericht warnt auch vor der zunehmenden Verbreitung intelligenter Kameras, die mithilfe biometrischer Daten Gesichter erkennen können. Etwa in Moskau, wo 100.000 solcher Geräte installiert worden seien, um die Einhaltung von Quarantäne-Verordnungen zu überwachen. In China seien Menschen zu diesem Zweck in einigen Fällen sogar aufgefordert worden, Webcams in ihren Wohnungen und vor ihren Haustüren zu installieren.

Gemäß dem Bericht wird es „schwierig, wenn nicht unmöglich" sein, solche Instrumente zur Überwachung wieder außer Betrieb zu nehmen, nachdem das Virus bezwungen ist. Die Geschichte zeige, „dass neue staatliche Vollmachten für gewöhnlich die ursprüngliche Bedrohung überdauern". Zahlreiche problematische Entwicklungen hätten sich durch übereilte Maßnahmen auch in demokratischen Staaten gezeigt.

Im Rahmen der Erstellung des Berichts über die Netzfreiheit haben die Analysten 65 Länder untersucht, in denen insgesamt etwa 87% der weltweiten Internetnutzer leben. Der Zeitraum der Untersuchung war Juni 2019 bis Mai 2020. In einem Ranking dieser Länder sehen die Analysten Deutschland mit 80 von 100 möglichen Punkten im positiven Sinne auf dem vierten Platz. Den ersten belegt Island (95 Punkte). China landet mit zehn Punkten das sechste Jahr in Folge auf dem letzten Platz. In die Bewertung fließt unter anderem auch ein, wie große Teile der Bevölkerung Zugang zum Internet haben und wie gut Menschenrechte online geschützt werden.

Bericht des Europarats

Ein Bericht des Europarats, der 55 europäische, lateinamerikanische und afrikanische Regierungen auf die Überwachungsfolgen der Corona-Pandemie untersucht, kommt zu ähnlichen Ergebnissen. Der Europarat mit Sitz in Straßburg ist eine europäische internationale Institution, der 47 Mitgliedsstaaten angehören. Er hat sich die Förderung des wirtschaftlichen und sozialen Fortschritts zur Aufgabe gemacht und kümmert sich um Fragen der demokratischen Sicherheit, darunter die Einhaltung der Menschenrechte. Untersucht wurden in dem Bericht die Staaten, die das seit 1985 geltende Datenschutzübereinkommen „Konvention 108" unterschrieben haben. Dem gemäß wurde trotz Warnungen des Europarats zu den Tracing-Apps bereits im Frühjahr 2020 das Übereinkommen der Konvention 108 von den Unterzeichnerstaaten nicht so genau genommen. Der Europarat hatte angesichts von Planungen zu Contact-Tracing-Apps zur Kontaktverfolgung Covid-19-Infizierter darauf hingewiesen, das Gebot der Datensparsamkeit zu beachten. Die informationelle Selbstbestimmung der Bürger dürfte nicht beeinträchtigt werden.

Im Bericht „Digital Solutions to fight COVID-19" analysiert der Europarat die von den Einzelstaaten mittlerweile getroffenen Gesetze und erstellten Tracing-Apps. Bemängelt werden vom Europarat mangelnde Gesetzesgrundlagen für die Maßnahmen und in einigen Fällen konkrete Verstöße gegen das Datenschutzübereinkommen. So haben beispielsweise Slowenien, Griechenland und Ungarn Patientenlisten mit der Polizei und Gesundheitsbehörden geteilt. Andere Staaten haben Daten von Patienten oder kürzlich Verstorbenen nur teilweise anonymisiert.

Der Bericht kritisiert, dass entgegen mehrfacher Aufforderungen des Europarats kompatible Systeme in Europa zu implementieren, Staaten eigene, ganz unterschiedliche Maßnahmen ergriffen haben. Durch die mangelnde Interoperabilität der Tracing-Apps und die fehlende Koordination sei die Wirksamkeit der Kontaktverfolgung, Selbstdiagnose und Durchsetzung der unterschiedlichen Corona-Maßnahmen schlecht ausgefallen (Bovermann, Selfies für den Staat, SZ 15.10.2020, 15; Dehling, Europarat: Datenschutzmängel bei Corona-Maßnahmen der Konvention-108-Staaten, www.heise.de 13.10.2020, Kurzlink: https://heise.de/-4926844).

Weltweit

Datenbanken im Internet oft ungenügend geschützt

Gemäß einer Untersuchung von NordPass ist das Internet voll von exponierten Datenbanken. Deutschland steht dabei weltweit an vierter Stelle. Aufgefunden wurden hier 361 ungesicherte Datenbanken mit 248.252.244 Einträgen, darunter befinden sich auch persönliche Daten wie E-Mails, Passwörter und Telefonnummern. Insgesamt wurden in 20 Ländern 9.517 ungesicherte Datenbanken mit 10.463.315.645 Einträgen gefunden.

Die Liste wird von China angeführt. Dort fand man fast 3.794 exponierte Datenbanken. Das bedeutet, dass 2.629.383.174 Konten von Nutzern gefährdet sind. An zweiter Stelle befinden sich die Vereinigten Staaten mit fast 3.000 ungesicherten Datenbanken und knapp 2,3 Milliarden online verfügbaren Einträgen. Mit 520 ungesicherten Datenbanken und 4.878.723 Einträgen befindet sich Indien an dritter Stelle.

Einige dieser Daten haben vielleicht keinen großen Nutzen und taugen nur zu Testzwecken. Einige davon können dagegen großen Schaden anrichten, wenn sie offengelegt werden. Einige der größten Datenlecks des letzten Jahres resultierten aus offengelegten Datenbanken. So waren zum Beispiel Millionen Facebook-Datensätze auf einem öffentlichen Amazon Server zugänglich. Bei einem anderen Vorfall wurden durch eine ungesicherte Datenbank Informationen von 80 Millionen Haushalten in den USA enthüllt. Bei den Daten ging es um die Adressen der Familien, das Einkommen und den Familienstand. Ein weiteres Datenleck gab es in einer Rehabilitationsklinik in den USA. Dort wurden fast 150 000 private Patientendaten preisgegeben.

Die Daten werden oft nicht durch einen erfahrenen Hacker offengelegt, sondern tauchen schlicht und einfach in einer öffentlichen Datenbank auf. Suchmaschinen wie Censys oder Shodan scannen das Internet ständig und machen es für jeden möglich, offene Datenbanken mit wenigen Klicks aufzuspüren. Wenn der Datenbank-Manager die Standard-Anmeldedaten verwendet, ist es ein Kinderspiel, diese zu herauszufinden, so Chad Hammond, Sicherheitsexperte bei NordPass: „Mit der richtigen Ausrüstung ist es möglich, das gesamte Internet in nur 40 Minuten selbstständig zu scannen." Datensicherheit und Datenschutz sollten oberste Priorität haben: „Jedes Unternehmen, jede Ins-

titution und jeder Entwickler sollte sicherstellen, dass Datenbanken niemals geknackt werden können, weil dies offensichtlich eine große Bedrohung für Nutzerdaten darstellt."

Die Hauptaspekte der Datenbanksicherheit sind laut Hammond „Datenverschlüsselung, Identitätsmanagement und Schwachstellenmanagement. Daten können sowohl während sie versendet werden als auch während der Zeit, in der sie ruhen, einem Risiko ausgesetzt sein. Deshalb müssen sie in beiden Fällen geschützt werden." Hierfür gibt es verschiedene Ansätze, aber die Verschlüsselung spielt beim Datenschutz eine tragende Rolle. Sie ist ein anerkanntes Mittel, um Daten sowohl bei der Übertragung als auch im Ruhezustand zu sichern. Alle Daten sollten durch die Nutzung starker und vertrauenswürdiger Algorithmen verschlüsselt werden, anstatt nur durch benutzerdefinierte oder zufällige Methoden. Die Wahl einer geeigneten Schlüssellänge sei wichtig, um das System vor Angriffen zu schützen.

Ein weiterer wichtiger Schritt ist demnach das Identitätsmanagement: „Damit kann sichergestellt werden, dass nur berechtigte Personen im Unternehmen Zugang zu technologischen Ressourcen haben. Jedes Unternehmen sollte ein Sicherheitsteam vor Ort haben, das für das Schwachstellen-Management verantwortlich ist und Sicherheitslücken frühzeitig erkennen kann." Der Sicherheitsexperte machte erneut auf die Bedeutung eines sicheren Passworts aufmerksam: „Die Tatsache, dass uns mehr als 10 Milliarden Passwörter zur Verfügung stehen, sollte die Leute dazu motivieren, lange und starke Passwörter zu wählen. Lautet Ihr Passwort ´12345´ kann auch die allerbeste Firewall Ihre Daten nicht mehr schützen. Ihr Passwort sollte auch kein Wort sein, das in einem Wörterbuch steht. Eine durchschnittliche Person verwendet nur etwa 20.000 bis 30.000 Wörter. Es kann also sein, dass alle bereits zu diesen 10 Milliarden gehören."

NordPass arbeitete mit einem White-Hat-Hacker zusammen, der Elasticsearch und mongoDB Bibliotheken nach exponierten, ungeschützten Datenbanken durchsucht hat. Wurde er fündig, loggte er sich in die öffentlich zugänglichen Datenbanken ein und überprüfte, welche Arten von Daten dort zu finden waren. Der Untersuchungszeitraum war Juni 2019 bis Juni 2020.

Die Rangliste:

China	3.794
USA	2.703
Indien	520
Deutschland	361
Singapur	355
Frankreich	247
Südafrika	239
Niederlande	149
Russland	148
Großbritannien	140
Südkorea	129
Irland	124
Vietnam	121
Hongkong	100
Brasilien	99
Japan	81
Kanada	78
Iran	47
Australien	46
Taiwan	36

(Über 248 Millionen persönliche Online-Zugangsdaten deutscher Internetnutzer offengelegt, www.all-about-security.de 30.07.2020).

Irland/Europa

Facebook wehrt sich gegen Datentransferverbot

Der Facebook-Konzern wehrt sich gegen das Verbot eines Transfers von Nutzerdaten in die USA, indem er die vorläufige Anordnung der irischen Datenschutzbehörde, die Datenübertragung abzustellen, vor dem obersten Gericht des Landes angefochten hat. Die Beschwerde gegen die irische Data Protection Commission wurde am 10.09.2020 eingereicht. Facebook wirft den Datenschützern vor, ohne eine Empfehlung der Datenschützer auf EU-Ebene gehandelt zu haben: „Ein Fehlen von sicheren und legalen internationalen Datentransfers hätte schwerwiegende Konsequenzen für die europäische Wirtschaft. Wir fordern die Regulierungsbehörden auf, eine pragmatische und angemessene Herangehensweise zu wählen, bis eine nachhaltige, langfristige Lösung erreicht werden kann."

Die irische Datenschutzbehörde lehnte eine Stellungnahme ab. Für den US-Konzern, der seinen Firmensitz in Europa in Irland hat, ist das eine operative und rechtliche Herausforderung, die einen Präzedenzfall für andere Technologiegiganten schaffen könnte. Die irische Behörde setzt mit ihrer Anordnung eine Entscheidung des Europäischen Gerichtshofs (EuGH) vom 16.07.2020 über Datentransfers durch (DANA 3/2020, 199 ff.). Dieses Urteil schränkte die Weitergabe von persönlichen Informationen über Europäer durch Unternehmen wie Facebook an den Mutterkonzern in den USA ein, da Europäer keine wirksame Möglichkeit haben, gegen eine Überwachung durch die amerikanische Regierung vorzugehen.

Die Datenschutzbehörde in Dublin hatte Facebook bis Mitte September 2020 Zeit gegeben, eine Antwort auf die vorläufige Anordnung zu geben. Danach soll ein Entwurf einer Anordnung an den Europäischen Datenschutzausschuss gehen. Ein Facebook-Sprecher sagte, dass man der Aufforderung fristgerecht nachkommen wolle (Facebook wehrt sich gegen das Verbot eines Transfers von Nutzerdaten in die USA, www.finanzen.net 11.09.2020).

Dänemark

Auslandsgeheimdienst FE bespitzelt dänische Bürger

Dänemarks sozialdemokratische Verteidigungsministerin Trine Bramsen hat den Chef des Militär- und Auslandsgeheimdiensts des Landes „Forsvarets Efterretningstjeneste" (FE) und drei leitende Mitarbeiter suspendiert. Hintergrund sind Untersuchungen auf Basis von Dokumenten, die Whistleblower an die Aufsichtsbehörde Tilsynet med Efterretningstjenesterne (TET) übergeben haben. Demnach wurden von dem Geheimdienst nicht nur widerrechtlich dänische Staatsbürger ausspioniert und die dabei gesammelten Daten auch weitergegeben. Der nun suspendierte Geheimdienstchef Lars Findsen soll außerdem Informationen vor der Aufsichtsbehörde zurückgehalten und falsche Angaben gemacht haben. Ein anderer Suspen-

dierter ist Findens Vorgänger, Thomas Ahrenkiel, der den Geheimdienst von 2010 bis 2015 geleitet hatte. Eigentlich sollte Ahrenkiel am 01.09.2020 als neuer Botschafter Dänemarks in Berlin sein Amt antreten. Daraus wurde nun nichts. Ministerpräsidentin Mette Frederiksen erklärte, sie nehme die Vorwürfe „sehr sehr ernst".

Die für die Überwachung der Geheimdienste zuständige Aufsichtsbehörde TET hatte am 24.08.2020 mitgeteilt, dass sie im November 2019 Dokumente zu Fehlverhalten beim FE erhalten hatte. Der Dienst ist für die Sammlung von Informationen im Ausland zuständig, die die nationale Sicherheit Dänemarks und der dänischen Truppen betreffen. Die Aufseher haben die Dokumente nach eigenen Angaben geprüft und nun Empfehlungen formuliert. Geprüft werden sollte demnach, ob sich der Geheimdienst an die geltenden Gesetze gehalten hat und ob die Verantwortlichen wahrheitsgemäß über die Überwachungsfähigkeiten informiert wurden. Außerdem sollten Whistleblower besser geschützt werden.

Der FE ist mit einem Budget von jährlich einer Milliarde Kronen (ca. 130 Mio. €) Dänemarks best ausgestatteter Geheimdienst. FE soll Dänemark vor internationalem Terrorismus und Cyberangriffen schützen und beobachtet das geopolitische Ringen in der Arktis ebenso wie die Herausforderungen durch Russland und China. Das Gesetz erlaubt FE-Spionen im Interesse Dänemarks „Ausländer zu überwachen und zu hintergehen". Dem Dienst ist es aber gemäß der dänischen Zeitung Politiken untersagt, „seine enorme Macht zu missbrauchen, um diejenigen illegal zu überwachen, die sie schützen sollen – die dänischen Bürger".

Das vierseitige Dokument der Aufsichtsbehörde enthält keine konkreten Angaben zu den Vorwürfen. Beobachter in Dänemark weisen bereits darauf hin, dass wegen der sensiblen Natur der Arbeit des Geheimdienstes nicht viel an die Öffentlichkeit dringen dürfte. Insgesamt erinnern die Vorwürfe aber an verschiedene Geheimdienstskandale der vergangenen Jahre – allen voran die Snowden-Enthüllungen im Jahr 2013 – nur hatten diese selten vergleichbare Konsequenzen. Der Nachrichtendienst FE stand 2017 schon einmal in der Kritik der TET. Schon damals hieß es, Staatsbürger seien illegal ausspioniert worden. Der FE hatte die Vorfälle stets so erklärt, dass es sich dabei um unabsichtlichen Beifang von Auslandsoperationen gehandelt habe. Im aktuellen Bericht ist erstmals davon die Rede, dass der Dienst Spionage gegen Dänen absichtlich und systematisch betrieben hat. Der FE soll gar eine Akte über ein Mitglied der Geheimdienstaufsicht selbst angelegt haben. Dies ist für den Politologen Malte Froslee Ibsen „schockierend".

Ein Großteil des Materials, das zur Enthüllung geführt hat, ist als geheim eingestuft. Die Presse begrüßte es, dass die Verfehlungen offiziell bekannt gemacht wurden und vier hochrangige Verantwortliche dafür suspendiert worden sind. Es wurde darauf verwiesen, dass die Enthüllungen allein den anonymen Whistleblowern zu verdanken seien. Es begann eine Debatte über die Rolle der Geheimdienstaufsicht.

TET war 2014 als unabhängige Behörde eingerichtet worden, um dafür zu sorgen, dass die im Zuge der Terrorbekämpfung zunehmend mächtigen Geheimdienste sich innerhalb der für sie demokratisch festgelegten Regeln und Gesetze bewegen. Die Aufsicht wurde oft als zahnlos kritisiert. Bei TET arbeiten fünf gewählte Mitglieder mit einem Stab von acht Mitarbeitern und einem Jahresbudget von umgerechnet 1,13 Mio. €. Die Zeitung Politiken kommentierte, es gebe ein „grobes Missverhältnis" zwischen der Stärke der Kontrolleure und der Geheimdienste. Man brauche sich nicht wundern, dass die Aufsicht „in all den Jahren hinters Licht geführt wurde".

Der TET-Bericht fordert das Parlament auf, schnellstmöglich ein Whistleblower-Programm für Geheimdienstmitarbeiter einzurichten. Die Politiker sollten prüfen, ob die Geheimdienstaufsicht tatsächlich „über die erforderlichen Kompetenzen und Ressourcen verfügt". Verteidigungsministerin Bramsen erklärte, sie werde umgehend eine unabhängige Untersuchung der Vorwürfe einleiten. Finden wies die gegen ihn vorgetragenen Vorwürfe zurück und nahm seine Mitarbeiter in Schutz: Sie hätten die nun erhobenen Anschuldigungen „nicht verdient". Der jetzt suspendierte Finden ist seit 2015 Chef des Geheimdiensts. Vorher hatte er auch schon mehrere Jahre den Inlandsgeheimdienst PET geleitet. Verteidigungsministerin Bramsen versicherte, dass sie die Angelegenheit mit größtem Ernst betrachte: „Es ist wichtig, dass wir darauf vertrauen können, dass unsere Geheimdienste im Rahmen ihrer Befugnisse agieren".

Die Reaktionen reichen von Fassungslosigkeit bis Zorn. Die rot-grüne Einheitsliste, welche die sozialdemokratische Minderheitsregierung unterstützt, sprach von einem „möglichen Angriff auf die dänische Demokratie". Die rechtspolitische Denkfabrik Justitia warnte vor einem „Staat im Staate". Der Politikwissenschaftler Ibsen sieht in dem Vorgang einen „historischen Vertrauensbruch". Nach allem, was bislang ans Licht gekommen sei, sei das Verhalten des FE „einer Bananenrepublik" würdig (Holland, Illegale Überwachung und Vertuschung: Dänischer Geheimdienstchef suspendiert, www.heise.de 25.08.2020, Kurzlink: https://heise.de/-4878099; Strittmatter „Einer Bananenrepublik würdig", SZ 26.08.2020, 7).

Großbritannien

20 Mio.-Pfund-Datenschutzstrafe gegen British Airways

Die britische Datenschutzbehörde, das Information Commissioner's Office (ICO), hat gegen British Airways (BA) ein Bußgeld in Höhe von 20 Millionen Britische Pfund wegen Verstößen gegen Gesetze zum Absichern der Privatsphäre von Kunden und Mitarbeitern verhängt. Dies entspricht umgerechnet rund 22 Millionen €. Das ICO wirft der Fluggesellschaft vor, „eine erhebliche Menge an persönlichen Daten ohne angemessene Sicherheitsmaßnahmen verarbeitet zu haben". In Folge sei es zu einer Cyberattacke gekommen, die das Unternehmen über zwei Monate lang nicht entdeckt habe (DANA 4/2018, 210 f.).

2019 hatte das ICO noch erklärt, die Strafe auf etwa 204 Millionen Euro festlegen zu wollen, was 1,5% des Umsatzes der BA im vorangegangenen Geschäfts-

jahr weltweit entsprochen hätte (DANA 3/2019, 161). Gemäß der Datenschutz-Grundverordnung (DSGVO), auf deren Basis die Aufsichtsbehörde das Verfahren einleitete, wäre eine Höchststrafe von bis zu 4% der Geschäftssumme möglich gewesen. Dass die Buße nun deutlich geringer ausfällt, begründet das ICO mit aktuellen Umsatzeinbußen bei BA durch die Corona-Pandemie. Man habe zudem weitere Einwände des Konzerns gegen den ursprünglichen Berechnungsansatz berücksichtigt.

Bei dem Angriff 2018 hatten Cyberkriminelle potenziell Zugriff auf persönliche Daten von rund 429.612 Kunden und Belegschaftsmitgliedern. Dies schloss die Namen, Adressen und Kreditkarteninformationen inklusive der Sicherheitscodes des Card Validation Value (CVV) von 244.000 Kunden mit ein. Dazu kamen Nutzernamen und Passwörter von Mitarbeitern wie Administratoren sowie von Inhabern von Premium-Vielflieger-Karten. Die ICO-Ermittler meinten, das Unternehmen hätte die Sicherheitslücken früher entdecken und schließen müssen. Dazu hätten gängige Schutzmaßnahmen wie begrenzte Zugriffsrechte, Zwei-Faktoren-Authentifizierung und „gründliche Tests" der Infrastruktur ausgereicht. Einige der Vorkehrungen wären über Einstelloptionen des Microsoft-Betriebssystems verfügbar gewesen, das BA genutzt habe. Allerdings habe die Firma ihre IT-Sicherheit nach der Attacke erheblich verbessert.

Die britische Datenschutzbeauftragte Elizabeth Denham betonte, dass es sich um die höchste Strafe handle, die das ICO bislang verhängt habe. Die Fluggäste hätten BA ihre persönlichen Daten anvertraut, die Versäumnisse zu deren Schutz seien „inakzeptabel" und hätten viele Betroffene verunsichert. Da die Panne im Juni 2018 erfolgte und damit zu einem Zeitpunkt vor dem Brexit, untersuchte das ICO den Fall nach eigenen Angaben im Namen des Europäischen Datenschutzausschusses (EDSA) als federführende Aufsichtsbehörde im Rahmen der DSGVO. Die Sanktionen seien über den gängigen Kooperationsprozess vom EDSA genehmigt worden. Das britische Datenschutzrecht orientiert sich an der DSGVO, auch wenn der britische Premierminister Boris Johnson dies ändern will (Krempl, Datenschutzpanne: British Airways muss 22 Millionen Euro zahlen – statt 204, www.heise.de 17.10.2020, Kurzlink: https://heise.de/-4931253).

Schweiz

Behörden diskutieren über Drohneneinsätze

In einem Bericht an den Grossen Rat der Stadt setzt sich der Datenschutzbeauftragte von Basel-Stadt Beat Rudin mit der Frage auseinander, ob öffentliche Organe Drohnen verwenden dürfen. Der Einsatz von Polizei-Drohnen bei Demonstrationen ist rechtlich nicht eindeutig geregelt. Die Bestimmung sei „technologieneutral" formuliert. Das Problem mit der Drohne sei, dass es sich dabei nicht einfach um eine Weiterentwicklung von Kameras handle. Sie erlaube „einen speziellen, eigenen Blick auf das Geschehen, ohne dass notwendigerweise ersichtlich ist, von wo die Aufnahme gemacht wird".

§ 58 des Polizeigesetzes (PoIG) des Kantons Basel-Stadt regelt: „Die Kantonspolizei kann aus Gründen der Beweissicherung Teilnehmerinnen oder Teilnehmer einer öffentlichen Veranstaltung aufnehmen, sofern die konkrete Gefahr besteht, dass Straftaten begangen werden." Rudin weist darauf hin, dass ohne entsprechende gesetzliche Grundlage nicht verdeckt gefilmt werden darf: „Dass unklar ist, wer von wem und von wo aus mit einer Drohne gefilmt wird, geschieht bei dieser Technologie sehr schnell." Nicht nur die informationelle Selbstbestimmung sei gefährdet, sondern auch die Versammlungsfreiheit. Dieses Grundrecht müsse von filmenden Beamten respektiert werden, zumindest so lange es keinen Hinweis auf einen Straftatbestand gebe.

Der Überwachungsparagraf ist gemäß dem Bericht eine „politisch heikle Materie". Es sei daher zu empfehlen, Aufnahmen auf „mit hoher Wahrscheinlichkeit strafrechtlich relevantes Verhalten" zu beschränken. Sobald Personen identifizierbar sind, werden die Daten zu Personendaten. Bei hochaufgelösten Aufnahmen einer Kundgebung auch von oben entstehen leicht Daten zu Personen, die in keinem strafrechtlichen Zusammenhang stehen.

Diverse Polizeien und Rettungsdienste in der Schweiz erwägen, Einsätze durch Drohnen zu ergänzen. In Luzern wurden Drohnen bereits bei der Baupolizei geprüft, konnten jedoch aufgrund mangelnder gesetzlicher Grundlage nicht eingesetzt werden. Toprak Yerguz, Mediensprecher der Kantonspolizei Basel-Stadt, erklärte, es seien bereits Testflüge mit Drohnen gestartet worden; allerdings seien bisher keine operativen Einsätze geplant, bis eine gesetzliche Grundlage vorhanden sei. An einer solchen werde aber derzeit gearbeitet.

Für Drohnen, die über 500 Gramm wiegen, ist es laut dem Schweizer Bundesamt für Zivilluftfahrt (Bazl) verboten über Menschenmengen zu fliegen. Der Begriff Menschenmenge wird dabei als Personengruppe mit mindestens 24 eng beieinander stehenden Personen definiert. Eine solche Drohne müsse mindestens 100 Meter von der Gruppe entfernt sein (Kolb, Darf die Polizei Demos mit Drohnen überwachen? www.20min.ch 04.09.2020).

Finnland

Hacker erpresst mit Psycho-Aufzeichnungen

Ein Unbekannter, der sich „ransom_man" nennt, schickte an Tausende Patienten des Psychotherapie-Unternehmens Vastaamo Erpresser-Mails. Darin drohte er: Entweder sie bezahlen 200 Euro in digitaler Währung an eine anonyme Bitcoin-Adresse, oder der Hacker veröffentlicht die Aufzeichnungen der vertraulichen Gespräche im Internet, die diese mit ihren Therapeuten und Therapeutinnen geführt haben und aus denen ihre intimsten Gedanken zu entnehmen sind.

Die gehackte Firma Vastaamo betreibt rund 20 Kliniken im ganzen Land. Dem finnischen IT-Sicherheitsspezialisten Mikko Hyppönen zufolge wurden die Daten bereits Ende 2018 aus einer internen Datenbank gestohlen: „Das sind keine Hacker, das sind moralisch degenerierte Psychopathen. Diese Menschen haben kein Mitgefühl." Der Hacker versuchte zunächst, das Unternehmen

selbst zu erpressen. 40 Bitcoin wollte er von Vastaamo, umgerechnet etwa 450.000 Euro. Als Vastaamo nicht zahlte, änderte der Erpresser Mitte Oktober 2020 seine Taktik und verschickte rund 40.000 Droh-Mails an alle Patienten.

Erpressung im Medizinbereich macht immer mehr Schule. Kurz vor dem Vorgang in Finnland war eine Frau in Düsseldorf auf dem Weg in ein weiter entferntes Krankenhaus gestorben, weil eine näher gelegene Notaufnahme mit Ransomware zu kämpfen hatte. Einer der vom finnischen Hack Betroffenen ist der IT-Sicherheitsexperte Sami Laiho. Er sei ein Opfer des Hacks, schrieb er für die ganze Welt lesbar auf Twitter: „Ich wollte, dass die Leute sehen, dass so was auch IT-Experten wie mir passieren kann." Laiho ist schockiert, nicht so sehr wegen seiner eigenen Daten, sondern wegen der wirklich verletzlichen Gruppen: „Ich war ein einziges Mal bei einem Therapiegespräch, wenn der Inhalt rauskommt, was soll's. Aber da sind auch Daten von Kindern und von Leuten, die jahrelang zu Therapien gingen."

Digitale Erpresserbanden zeichnen von sich selbst gern das Bild von Geschäftsleuten, die eher zufällig auf der falschen Seite des Gesetzes stehen. Tatsächlich ähneln sie oft Unternehmen, ihre Raubzüge sind strukturierter und arbeitsteiliger als die von normalen Einbrecherbanden. Am Anfang der Entwicklung von digitaler Erpressung standen innovative Kleinkriminelle, die Privatrechner verschlüsselten und ein paar Hundert Euro Lösegeld wollten, damit sie die Familienfotos wieder freigaben. Bald übernahmen Profis das Geschäft. Im Zentrum der Attacken standen nun Firmensysteme. Unternehmen haben mehr finanzielle Mittel als Privatleute, um hohe Lösegelder zu zahlen. Gleichzeitig ist ihr Leidens- und damit Zahlungsdruck höher, wenn die Firma sonst pleitegeht. Im Jahr 2019 gingen Angreifer dazu über, Daten der Opfer nicht nur zu verschlüsseln, sondern auch zu stehlen. Auf Leak-Seiten im Darknet werden dann private, gerne pikante Daten von CEOs sowie Firmengeheimnisse hochgeladen. Das erhöht den Druck, sollten sich die Unternehmen weigern zu zahlen. Auch vom Vastaamo-Hack wurden bereits einige Patientendaten ins Netz gestellt. Für den Cybercrime-Experten Jeremy Kenelly von der US-Firma Fireeye kommt diese Entwicklung nicht überraschend: „Die Angreifer wollen nicht höflich sein, sie wollen Geld verdienen." In Finnland ist nach dem Vastaamo-Hack die Wut groß. Gemäß Hyppönen ist jetzt jeder IT-Experte des Landes hinter den Erpressern her. Es ist aber unsicher, ob der Angreifer je gefunden wird. Die Kombination aus verschlüsselter Internetverbindung und Zahlung in Bitcoin hilft den Kriminellen. Solange sie keinen Fehler machen, ist Cyber-Erpressung ein relativ sicheres Geschäftsmodell.

Was mit der betroffenen Firma Vastaamo passiert, ist indes unklar. Dass die Daten wohl nicht ausreichend gesichert waren, ist naheliegend. Am 26.10.2020 feuerte Vastaamo seinen CEO; die Behörden beschlagnahmten Teile von dessen Privatvermögen. Er hatte offenbar seit über einem Jahr von einem Hack gewusst, und zwar auch schon zu dem Zeitpunkt, als er das gut laufende Unternehmen für viel Geld an Investoren verkaufte (Muth, Willkommen in der Dystopie, SZ 29.10.2020; „Diese Menschen haben keinerlei Mitgefühl", www.sueddeutsche.de 29.10.2020).

USA

Rücksichtsloser digitaler Präsidentschaftswahlkampf

Bei der Präsidentschaftswahl 2008 in den Vereinigten Staaten wurde Barack Obama nicht nur wegen seiner Ideen für Amerika als Visionär gefeiert, sondern auch für seinen Umgang mit dem Internet. Der Kandidat hatte als Teil seiner Wahlkampagne ein eigenes soziales Netzwerk gestartet. Auf my.barackobama.com konnten sich Wähler und Unterstützer untereinander vernetzen, Veranstaltungen planen oder sich als Wahlhelfer registrieren. Manch normaler Wähler fühlte sich so mit seinen Sorgen und Nöten ernst genommen und angesprochen. Über diese Art von Wahlkampf von den Massen für die Massen hieß es, Obamas Kampagne hole die Menschen zurück in den politischen Prozess. Was damals als revolutionär galt, wirkt im Rückblick eher niederschwellig. Knapp acht Millionen Dollar gab Obama im gesamten Verlauf der Kampagne für Werbung im Internet aus, etwa 500.000 davon gingen an Facebook.

2020 investierten die Kandidaten innerhalb einer einzigen Woche das Zehnfache. Gemäß Schätzungen kostet Joe Biden und Donald Trump ihre Kandidatur insgesamt elf Milliarden Dollar. Ein immer größerer Teil wird in digitale Wahlwerbung investiert. In den letzten Wochen vor der Wahl schalteten die Kampagnen so viele Anzeigen, dass selbst im vermeintlich grenzenlosen Internet der Platz knapp wurde.

Geändert hat sich nicht nur das Ausmaß der Investitionen, sondern auch die gesellschaftliche Wahrnehmung von Privatsphäre. Spätestens seit dem Skandal um das Datenanalyse-Unternehmen Cambridge Analytica im Jahr 2016 ist klar geworden, dass die ungehemmte Digitalisierung der politischen Kommunikation nicht nur Teilhabe ermöglicht, sondern dieselbe Unwucht in das Machtgefüge zwischen Absender und Adressat bringt, die auch in der Privatwirtschaft herrscht. Wahlwerbung ist in den USA kaum reglementiert. So stand den Kampagnen ein großes Arsenal von moralisch fragwürdigen Werbetechniken zur Verfügung, die nur noch bedingt mit Demokratie zu tun haben, seien es gezielte Werbung, Big-Data-Wähleranalysen oder übergriffige Apps.

Politisches Microtargeting

Es obliegt den Tech-Unternehmen zu entscheiden, was sie in ihren Domänen zulassen und was nicht. Google erlaubt beispielsweise keine zielgerichtete Werbung auf seinen Seiten, das sogenannte Microtargeting. Twitter sorgte mit der Ankündigung für Aufregung, Wahlwerbung auf seiner Plattform gänzlich zu unterbinden. Facebook blieb als wichtigstes Schlachtfeld übrig, auch wenn das Netzwerk gerade unter jungen Menschen immer weiter an Relevanz verliert. Wie jedem anderen Werbetreibenden stellte Facebook auch den Präsidentschaftskandidaten ein komplett automatisiertes System zur Verfügung. Sie kommunizierten also nicht mehr mit Menschen, die sie von ihrer Botschaft überzeugen wollen, sondern nur noch mit der Software, die

Facebooks Werbemaschinerie antreibt. Wer aus welchen Gründen welche Anzeige zu sehen bekam, war kaum noch zu durchschauen.

Grundlage der digitalen Kampagne waren die Daten der US-Bürger, die den IT-Unternehmen aber auch den beiden Parteien zur Verfügung stehen. In der amerikanischen Politik herrscht längst dieselbe Big-Data-Gläubigkeit, die auch in der Privatwirtschaft grassiert. Man muss, so die Annahme, nur genügend Informationen sammeln, um genau zu wissen, welchen Wähler man in welcher Situation mit welcher Botschaft ansprechen sollte. Dabei wird nicht mehr nur nach simplen soziodemografischen Merkmalen wie Geschlecht, Wohnort oder Alterskohorte sortiert, sondern nach Interessen und Lebensmodellen, die in ihrem Detailgrad obsessiv wirken. Ein alleinstehender Mann, der selbstständig und Waffenbesitzer ist, bekommt andere Botschaften zu sehen als liberale Paare in den Vorstädten.

Parteien auf den Abwegen der Kommerzunternehmen

Die Parteien unterhalten selbst große Datensilos, die einen reibungslosen Austausch der einzelnen Kampagnen und Kandidaten ermöglichen. Bei „Data Trust", der Datenbank der Republikaner, heißt es etwa, das „exklusive Dateninventar besteht aus einer tiefgreifenden Datensammlung von mehr als 300 Millionen Menschen, mit bis zu 2.500 Datenpunkten für jeden einzelnen". Die Republikaner nutzen ihre Datenbank bereits seit 2013. Die Konkurrenz von den Demokraten hat ihre eigene Version, die sogenannte „Democratic Data Exchange" erst im Laufe der Kampagne für den Wahlkampf 2020 gestartet, obwohl Hillary Clinton 2017 auch die mangelnde Datenausstattung für ihre Niederlage mitverantwortlich gemacht hatte.

Die persönlichen Kampagnen-Apps der beiden Kandidaten dienten nicht nur der Kommunikation und Partizipation, sondern auch dem Datensammeln. In den umfangreichen Berechtigungen, die Nutzer auf ihren Smartphones gewähren mussten, gleichen sie eher Schadsoftware. Joe Bidens App namens „Vote Joe" verlangt beispielsweise erst mal Zugriff auf die Kontakte im Telefon, gleicht diese Informationen mit bundesweiten Wählerdateien ab und filtert so Freunde und Bekannte nach politischer Orientierung und vergangenen Wahlentscheidungen.

Der Fachbegriff dafür heißt „Relational Organizing", was für deutsche Verhältnisse reichlich invasiv und inakzeptabel wäre, aber das ist in den USA noch längst nicht High-End. Alan Knitowski, dessen Unternehmen Phunware Trumps App entwickelt hat, prahlte, der Unterschied zwischen der Biden-App und dem Trump-Produkt ähnele dem zwischen einem gebrauchten Pick-up-Truck und einem Ferrari. Trumps App verlangte unter anderem auch Zugriff auf Bluetooth-Funkverbindungen und GPS-Signal. Sam Woolley, Professor für Propagandaforschung an der Universität von Texas, erläuterte: „Sie wollen wissen, ob man Sonntag in die Kirche geht oder auf den Schießstand oder zur Abtreibungsklinik. Und wenn Sie diese Informationen haben, können Sie das mit anderen Datenpunkten verbinden, um den Wähler mit personalisierter Werbung zu erreichen."

Von einem vermeintlichen Mittel zum politischen Engagement mutiert das Programm zu einem hocheffizienten Wählerüberwachungswerkzeug. Zum Einsatz kommen sämtliche Muster, mit denen auch die Privatwirtschaft versucht, ihre Angestellten und Konsumenten zu disziplinieren. Dazu gehört auch das Prinzip der Gamification: Wer seine Bekannten überzeugte, sich die Trump-App ebenfalls herunterzuladen, oder wer Telefondienst für die Kampagne leistete, bekam Punkte gutgeschrieben. Hatten sie einen gewissen Zwischenstand erreicht, bekamen App-Nutzer etwa einen Nachlass auf Fanartikel von Donald Trump mit dem „Make America Great Again"-Slogan.

Neben der Datenobsession wurden diesmal auch Influencer, die sonst eher Konsumgüter auf ihren Instagram-Kanälen anpreisen, eingesetzt, um Botschaften unters Volk zu bringen. Joe Biden ließ sich immer wieder von wohlgesinnten Promi-Nutzern interviewen, und Donald Trump hatte einen ganzen Chor an ultrakonservativen Multiplikatoren, die seine Tiraden nachbeteten. Der Einsatz von nicht gerade subtilen Social-Media-Persönlichkeiten ist zwar nicht sonderlich elegant, war aber wohl trotzdem ein unvermeidbarer Weg, um Zielgruppen anzusprechen, die mit Politik sonst kaum noch in Berührung kommen.

Big-Data-Prognostik

Auch die Wahlumfragen sind vom technischen Wandel nicht ausgenommen. Donald Trumps Erfolg 2016 hat schließlich nicht nur den Glauben an den gesunden Menschenverstand im Allgemeinen, sondern auch den von Wahlforschern und Demoskopen an ihre Erhebungen erschüttert. Herkömmlichen Befragungen macht unter anderem das Phänomen der sozialen Erwünschtheit zu schaffen. Das bedeutet, dass Menschen zwar Populisten wählen, dies aber nur ungern zugeben und den Wahlforschern aus Scham eine falsche Antwort geben.

Hoffnung macht insofern Polly, ein KI-Programm des kanadischen Start-ups Advanced Symbolics. Die Software umgeht das Problem, indem sie eine ungleich größere und trotzdem repräsentative Stichprobe in den sozialen Medien auswertet und mit eigenen Vorhersagemodellen abgleicht. Entgegen der Meinung sämtlicher menschlicher Experten sah Polly auch Trumps Sieg vor vier Jahren voraus. Seitdem hat das Programm mehr als 20 Wahlen weltweit korrekt vorhergesagt. Darunter auch eher unwahrscheinliche Entscheidungen wie etwa den Brexit oder eine Minderheitsregierung in Kanada. Auch 2020 war die KI sich ziemlich sicher: Eine Woche vor dem Stichtag prognostizierte sie einen Biden-Sieg mit 353 zu 185 Wahlleuten (Moorstedt, Sie haben keine Wahl, SZ 28.10.2020, 27).

USA

Verily sammelt Daten bei hoheitlichen Corona-Tests und ignoriert soziale Realität

Verily, eine Tochter des Alphabet-Konzerns, zu dem auch Google gehört, hat staatlich finanzierte Coronavirus-Tests in Kalifornien so aufgesetzt, dass diese nur mit Gmail-Konto und Smart-

phone möglich sind, und nur, wenn man Gesundheitsdaten preisgibt und deren Weitergabe an unbekannte Dritte abnickt. Dabei sollte das 55 Millionen US-Dollar teure Projekt gerade Armen und anderweitig Unterversorgten zu den Tests verhelfen. Weil dieses Ziel so nicht erreicht wird, haben die Countys San Francisco und Alameda ihre Zusammenarbeit mit Verily eingestellt. Verily betreibt in etwa der Hälfte der 58 Countys Kaliforniens stationäre und mobile Coronavirus-Teststationen sowie eine Online-Plattform für die Terminvereinbarung. Partnerlabore übernehmen die Auswertung. Das System soll, so Kaliforniens Gouverneur Gavon Newsom im April 2020, „sicherstellen, dass wir wirklich Kalifornien testen, breit definiert – nicht nur Teile Kaliforniens und jene, die irgendwie das Privileg haben, bevorzugt zu werden".

Verily verlangt, dass jeder Testwillige ein Gmail-Konto verwendet. Verily begründet das mit der „Sicherheit". Außerdem muss jeder Teilnehmer chronische Krankheiten offenlegen, und dann zustimmen, dass die verpflichtend preisgegebenen Gesundheitsdaten auch an ungenannte Vertragspartner, Regierungsstellen und „andere Einrichtungen, die das Testprogramm unterstützen", weitergegeben werden dürfen. Wer das verweigert, bekommt über Verilys Plattform keinen Termin. Das schreckt insbesondere Angehörige der sowieso unterversorgten Zielgruppen ab. Sie bringen Behörden und Konzernen wenig Vertrauen entgegen, da sie schon zu oft von diesen schlecht behandelt, ignoriert, oder gar ausgeraubt wurden. Verily verteilte Schutzausrüstung wie Handschuhe und Masken, die für Arme unerschwinglich sind. Auch das gab es nur für jene, die ihre Daten hergegeben hatten. Dabei liegen die COVID-Raten gerade bei sozial Benachteiligten um ein Vielfaches über dem Durchschnitt.

Dr. Noha Aboelata, Chefin einer Klinik in Oakland, kommentierte das Vorgehen: „Für uns ist das eine alte Geschichte. Firmen, die sich nicht wirklich um unsere Gemeinde kümmern, stürmen mit Geschenken herein, aber was sie wieder mitnehmen, ist viel wertvoller." Sie meint die Gesundheitsdaten. Aboelata fand Verilys Zugang so unwürdig, dass sie die Zusammenarbeit mit Verily nach nur sechs Tagen wieder eingestellt hat. Dazu trug auch bei, dass Verily die Teststation als Drive-In bewarb, obwohl sie, im Einklang mit den Bedürfnissen der lokalen Bevölkerung, für Fußgänger eingerichtet war. Die falsche Beschreibung lockte Wohlhabendere aus anderen Gegenden an, die dann wütend waren, weil sie ihr Vehikel parken und ein bisschen zu Fuß gehen mussten – in einem Armenviertel, wo sie, so Aboelata, wahrscheinlich noch nie waren und offenbar nicht sein wollten. Dies provozierte Konflikte so arg und geifernd, dass mehrere Menschen rausgeschmissen werden mussten.

Überraschend unflexibel erwies sich Verilys Terminvergabe. Frühestens am nächsten Tag kann man sich testen lassen. Das ist besonders frustrierend für Personen, die mangels eigenem Internetzugang zur Teststelle kommen, um sich dort online zu registrieren. Selbst wenn sich die Krankenschwestern gerade langweilen, müssen die Patienten an einem anderen Tag zu einer bestimmten Zeit wiederkommen, was für die Zielgruppe eine hohe Hürde ist. Im Stadtzentrum San Franciscos war zudem ein Smartphone Pflicht für die Terminvereinbarung vor Ort. Wer keines hatte, wurde weggeschickt – und kam damit auch um den versprochenen Einkaufsgutschein über zehn Dollar herum. Dass Leute mit Smartphone den Termin nicht vor Ort vereinbaren müssten, sondern dafür ihr Smartphone nutzen könnten, spielte keine Rolle.

Viele sozial Benachteiligte haben durchaus ein Gmail-Konto und würden es auch verwenden. Doch ein Gutteil hat das Passwort vergessen, weil Menschen ohne Internet selten das Passwort brauchen. Google setzt für die Passwortrücksetzung voraus, dass der Kontoinhaber entweder das Passwort eines anderen, dereinst hinterlegten E-Mail-Kontos kennt, oder dass er noch dieselbe Telefonnummer wie bei Einrichtung des Gmail-Kontos hat. Auch das ist eine weltfremde Forderung für die Zielgruppe.

Zu allem Überdruss verlangt Verily, dass Testwillige alle Angaben selbst machen. Hilfe Dritter ist unzulässig. Gleichzeitig stellt Verily die Anmeldung ausschließlich auf Englisch und Spanisch zur Verfügung. Verily geht also davon aus, dass alle Kalifornier ausreichend lesen und schreiben können, um Fragen nach Krankheiten schriftlich beantworten und Datenschutzbestimmungen verstehen und akzeptieren zu können. Dabei ist bekannt, dass die Hälfte aller US-Amerikaner nicht in der Lage ist, für die achte Schulstufe vorgesehene Bücher zu lesen. Und unter allen US-Staaten hat Kalifornien mit 23,1% die höchste Analphabetenrate, wobei der Anteil unter sozial Benachteiligten noch höher ist. Auch das erklärt, warum eine Terminvergabe für einen anderen Tag eine Hürde darstellt: Der Testwillige muss Datum und Uhrzeit korrekt ablesen und sich einprägen.

Von Kundenorientierung ist auch nach erfolgtem Test wenig zu sehen. Nur bei positivem Testergebnis versucht ein Callcenter, den Virusträger anzurufen. Wer nicht online Nachschau halten kann, bleibt im Unklaren, ob er COVID-negativ ist, das Testergebnis noch nicht vorliegt, oder ob ihn das Callcenter bloß nicht erreicht hat. In Teilen Kaliforniens ist Verilys Plattform der einzige Weg, zu einem COVID-Test zu kommen. In mehreren anderen US-Staaten arbeitet Verily mit der Apothekenkette Rite Aid zusammen. Für die Abwicklung des Rite-Aid-Testprogramms zahlt das US-Gesundheitsministerium 122,6 Millionen US-Dollar (Sokolov, COVID-Tests: Google-Schwester Verily ignoriert Lebensrealität Armer, www.heise.de 29.10.2020, Kurzlink: https://heise.de/-4941959).

USA

Verfassungsrechtliche Zweifel an unbestimmter Funkzellenabfrage

In den USA haben Richter eines Bundesgerichts den Antrag der Ermittlungsbehörden zur Genehmigung einer Funkzellenabfrage mehrfach abgewiesen und dabei verfassungsrechtliche Bedenken angeführt. Die Entscheidungen der Richter sind bemerkenswert, weil sie das in den USA übliche Verfahren für Funkzellenabfragen in Frage stellen. In dem Ermittlungsverfahren wegen Arzneimitteldiebstahl hatten Behörden in Chicago eine gerichtliche Anordnung beantragt, um Google zur

Herausgabe von Standort- und Nutzerdaten zu zwingen. Die Behörden wollten Angaben über Identifikationsnummern und Standortdaten aller Smartphones, die sich zu verschiedenen Terminen an bestimmten Orten aufgehalten hatten.

Für solche Datenherausgaben hat sich in den USA ein dreistufiges Verfahren etabliert. Im ersten Schritt sollte Google anonymisierte Daten der Geräte übermitteln, die zur fraglichen Zeit am fraglichen Ort waren. Aus dieser Liste wählen die Behörden dann bestimmte Geräte aus, über die sie weitere Informationen erhalten möchten. Für eine weitere Auslese des Gerätepools werden dann auch identifizierende Informationen über die Account-Inhaber angefordert.

Den Richtern in dem Chicagoer Verfahren war das aber zu unspezifisch. Sie sind der Ansicht, dass der Antrag angesichts der Zielregion im dicht besiedelten Stadtgebiet zu breit gefasst ist. Damit gerate er in Konflikt mit dem vierten Verfassungszusatz, der eine genaue Eingrenzung für Überwachungs- und Durchsuchungsbefehle verlangt. Es gebe zwar hinreichenden Grund zu der Annahme, dass ein Mobiltelefonnutzer innerhalb der eingegrenzten Gebiete ein Verbrechen begangen haben könnte, räumte Bundesrichter David Weisman in einer ersten Ablehnung des Antrags ein. Doch sei nicht ausreichend begründet worden, warum alle anderen betroffenen Geräte ebenfalls mit dem Verbrechen in Verbindung stünden. Der Zielbereich des Antrags sei nicht „eng zugeschnitten", wenn in einer belebten Stadt der Großteil der Erfassten „überhaupt nichts mit den untersuchten Straftaten zu tun" habe. Weisman kritisiert zudem, dass „die undisziplinierte und übertriebene Anwendung" der Funkzellenabfragen die „Privatsphäre und das Vertrauen in Strafverfolgungsbeamte gefährdet". Laut Google war die Zahl der Abfragen im Jahr 2018 gegenüber 2017 um 1.500% gestiegen.

Nach der Abweisung ihres Antrags hatten die Behörden einen geänderten Antrag gestellt, in dem die Zielregion leicht verkleinert wurde. Ein zweiter Richter, Gabriel Fuentes, lehnte auch dieses Ersuchen ab. Die Ermittler versuchten es ein drittes Mal und schlugen vor, auf den dritten Schritt der Identifikation verdächtiger Konten zu verzichten. Fuentes ging darauf aber nicht ein, da die Verwaltung zugab, dass sie eine separate Anordnung verwenden könnte, um an die detaillierten Nutzerinformationen zu gelangen.

Fuentes verweist zudem auf eine Entscheidung des Supreme Courts, wonach ein Durchsuchungsbefehl für eine Bar und einen dort Angestellten der Polizei nicht die Befugnis gab, jede Person zu durchsuchen, die sich zufällig in der Örtlichkeit aufhielt. Diese Ansage lasse sich analog auf das aktuelle Verfahren beziehen (Krempl, Funkzellenabfrage: US-Bundesrichter stellen die Verfassungsfrage, www.heise.de 01.09.2020, Kurzlink: https://heise.de/-4883539).

Rechtsprechung

EuGH

DSGVO gilt im Parlaments-Petitionsausschuss

Gemäß einem Urteil des Europäischen Gerichtshofs (EuGH) vom 09.07.2020 haben Bürger, die beim Petitionsausschuss eines Landesparlaments eine Petition einreichen, ein Recht auf Auskunft personenbezogener Daten (Az. C-272/18). Die Petitionsausschüsse von Bundesländern fallen demgemäß unter die Regeln der EU-Datenschutz-Grundverordnung (DSGVO). Hintergrund ist ein Fall in Hessen, bei dem ein Bürger eine Petition eingereicht hatte und etwas über seine Daten wissen wollte. Der Landtag hatte dies mit der Begründung abgelehnt, das Parlament unterliege der DSGVO nicht (DSGVO gilt in Petitionsausschuss, www.hessenschau.de 09.07.2020).

EuGH

TK-Vorratsdatenspeicherung nicht völlig ausgeschlossen

Der Europäische Gerichtshof (EuGH) entschied mit Urteilen vom 06.10.2020, dass eine flächendeckende und pauschale Speicherung von Internet- und Telefon-Verbindungsdaten nicht zulässig ist (C-623/17, C-511/18, C-512/18, C-520/18). Ausnahmen bei der Übermittlung und Speicherung von Verbindungsdaten seien aber möglich zur Bekämpfung schwerer Kriminalität oder im Fall einer Bedrohung der nationalen Sicherheit. Davon sind alle Nutzer der Dienste betroffen, auch wenn diese in keiner Hinsicht verdächtig sind, solche Verbrechen begangen zu haben oder zu begehen.

Der Gerichtshof hält in seinen Urteilen explizit fest, dass das europäische Recht, insbesondere die in diesem Fall gültige Richtlinie zur Privatsphäre in der elektronischen Kommunikation, nationale Gesetze ausschließe, die anlasslose pauschale Vorratsdatenspeicherung, pauschale Datenübertragung an Strafverfolger oder die Einschränkung der Privatsphären-Richtlinie zum Inhalt haben.

Die Richter bestätigten zwar, dass die flächendeckende und pauschale Speicherung der Verbindungsdaten nicht zulässig ist, ermöglichten aber Ausnahmen für die Bekämpfung schwerer Kriminalität und die konkrete Bedrohung der nationalen Sicherheit. Auch Standortdaten dürfen in diesen Fällen für Ermittler gespeichert werden. Sie verraten, wo sich eine Person wann aufgehalten hat.

Ausnahmen für das strikte Verbot der Speicherung und Übertragung von Ver-

bindungsdaten an Strafverfolger sind nach den Urteilen möglich, wenn EU-Mitgliedsstaaten sich etwa einer ernsten Bedrohung der nationalen Sicherheit gegenübersähen, die allgemein, aktuell und vorhersehbar sei. Das könnte zum Beispiel nach einem Terroranschlag der Fall sein. Allerdings dürften die Daten nicht länger als nötig gespeichert werden. Entsprechende Speicherungs- und Übermittlungsmaßnahmen müssen strikt auf den Anlass und seine Dauer begrenzt werden; sie müssen zudem durch ein Gericht oder eine unabhängige Institution jederzeit verbindlich überprüft werden können. Dabei müsste auch geprüft werden, ob tatsächliche eine so ernste Bedrohung vorliegt. Entsprechendes gilt auch für Maßnahmen gegen schwere Straftaten und bei Bedrohungen für die öffentliche Sicherheit. Generell hält der Gerichtshof fest, dass die Speicherung und Übermittlung von Verbindungsdaten immer auf den Anlass begrenzt sein muss und nur so lange zulässig ist, solange dieser Anlass auch gegeben ist. Der EuGH erlaubt aber, „eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen vorzunehmen". Die Internetkennungen ließen sich dann einfach über die Bestandsdaten der Provider einer konkreten Person zuordnen. Informationen, die sich „auf die zivile Identität der Nutzer" beziehen, dürften sogar ohne bestimmte Frist protokolliert werden.

Nationale Gerichte aus Frankreich, Belgien und Großbritannien hatten den EuGH als höchstes europäisches Gericht mit Sitz in Luxemburg um eine Einschätzung zu der Frage gebeten, ob einzelne EU-Staaten den Betreibern elektronischer Kommunikationsdienste hierzu allgemeine Pflichten auferlegen dürfen.

Diskussion in Europa

Der EuGH hat in dieser Runde Verfahren aus Frankreich, Belgien und Großbritannien behandelt. Weitere Klagen, die das aktuelle deutsche, derzeit ausgesetzte Gesetz zur Vorratsdatenspeicherung betreffen, sind noch anhängig. Christian Mihr, Geschäftsführer von Reporter ohne Grenzen in Deutschland, zeigte sich zuversichtlich, dass das Gericht auch hier klarstellen werde, dass eine solche „flächendeckende Vorratsdatenspeicherung nicht mit europäischem Recht vereinbar ist". Es sei höchste Zeit anzuerkennen, dass die deutschen Regeln gegen Grundrechte verstießen und den Quellenschutz infrage stellten. In Deutschland liegt die Vorratsdatenspeicherung auf Eis. Allerdings können aus den bisherigen Urteilen des EuGH sowie entsprechenden Entscheidungen des deutschen Bundesverfassungsgerichts (BVerfG) Schlüsse für die rechtliche Bewertung der bestehenden ausgesetzten Gesetze gezogen werden. Im aktuellen Fall erfolgten die EuGH-Vorlagen durch den belgischen Verfassungsgerichtshof, den französischen Staatsrat und das britische Gericht für Ermittlungsbefugnisse. Diese wollten u.a. wissen, ob die europäische Datenschutzrichtlinie für elektronische Kommunikation zum Beispiel auf Maßnahmen zur Terrorabwehr angewandt werden kann. Der Generalanwalt des EuGH, Manuel Campos Sánchez-Bordona, hatte im Januar 2020 betont, dass aus seiner Sicht auch dabei rechtsstaatliche Prinzipien gelten müssten.

Der EuGH hatte zuvor im Jahr 2016 entschieden, dass eine unterschiedslose Speicherung von Telefon- und Internetverbindungsdaten mit EU-Recht nicht vereinbar sei. Auch andere frühere Urteile, die eine generelle Speicherverpflichtung kritisch bewerteten, stießen bei Politikern in EU-Ländern auf Skepsis. Sie befürchten, dass Sicherheitsbehörden damit ein wichtiges Mittel zum Schutz der nationalen Sicherheit aus der Hand geben.

Die EU-Staaten hatten die EU-Kommission im Jahr 2019 damit beauftragt, trotz des EuGH-Urteils von 2016 die Möglichkeiten einer Vorratsdatenspeicherung auszuloten. Die Brüsseler Behörde soll nach einem Beschluss der Justizminister eine Studie für mögliche Lösungen und etwaige Gesetze vorlegen. Zudem will Deutschland, das in der zweiten Jahreshälfte 2020 die EU-Ratspräsidentschaft innehat, im Ministerrat eine neue Arbeitsgruppe einsetzen. Sie soll sich mit dem verdachtsunabhängigen Protokollieren von Nutzerspuren befassen.

Die Vorratsdatenspeicherung von Telekommunikationsdaten ist hoch umstritten: Während Sicherheitspolitiker in ihr ein zentrales Instrument im Kampf gegen organisierte Kriminalität, Kinderpornografie und Terrorismus sehen, halten Bürgerrechtler und Verbraucherschützer sie für riskant und überzogen. Die Unternehmen sind dabei gesetzlich verpflichtet, Telefon- und Internetverbindungsdaten der Nutzer zu sichern, so dass Ermittler später bei Bedarf darauf zugreifen können.

Gegner der Vorratsdatenspeicherung nehmen hingegen an, dass manche Schwerkriminelle und Terroristen ohnehin für sie passende Dienste oder Verschlüsselungstechniken einsetzen, die nicht mit Hilfe der Vorratsdatenspeicherung erfasst werden – am Ende würden dann vor allem die Daten unbescholtener Bürger erfasst.

Diskussion in Deutschland

In Deutschland wurden immer wieder Anläufe gemacht die Vorratsdatenspeicherung einzuführen, die dann ganz oder in Teilen vom BVerfG und/oder vom EuGH verworfen wurden. Die aktuell für Deutschland geltende Regelung ist seit einem Urteil von 2017 ausgesetzt. Dazu läuft ein eigenes Verfahren vor dem EuGH; wann ein Urteil fällt, ist unklar. Laut dem Gesetz sollten eigentlich Standortdaten von Handynutzern für vier Wochen gespeichert werden, angerufene Nummern, Uhrzeit und Dauer von Anrufen sowie Sende- und Empfangszeiten von SMS für zehn Wochen.

Zuletzt forderten die Justizminister von CDU und CSU, die Vorratsdatenspeicherung müsse so schnell wie möglich „wiederbelebt" werden. „Der Kampf gegen Kinderpornografie im Internet zeigt: Fehlende Verkehrsdatenspeicherung verhindert, dass wir Straftaten aufklären und noch laufenden Kindesmissbrauch stoppen können." Auch Bundesjustizministerin Christine Lambrecht (SPD) forderte, dass im Kampf gegen Kindesmissbrauch und pornografische Darstellungen von Gewalt gegen Kinder dieses Mittel genutzt werden kann: „Wir werden den Ermittlern auch die Möglichkeit an die Hand geben, die Vorratsdatenspeicherung zu nutzen, soweit dies mit deutschem und europäischem Recht vereinbar ist."

Gegen dieses Argument, das in der Diskussion um die Vorratsdatenspeicherung immer wieder zu hören ist, wendeten etwa Baden-Württemberg,

Bremen und Rheinland-Pfalz gegen eine Initiative Mecklenburg-Vorpommerns im Bundesrat ein, die Aufklärungsquote bei der Verbreitung von Darstellungen sexuellen Kindesmissbrauchs habe laut der Polizeilichen Kriminalstatistik bis 2019 auf 93,4 Prozent gesteigert werden können. Dies zeige, dass auch ohne das umkämpfte Instrument „Erfolge bei der Verfolgung von Kinderpornografie erzielt" würden. Der Fokus darauf lenke gar von „zielführenderen Möglichkeiten ab, Kinder besser vor sexualisierter Gewalt zu schützen". Auch die jüngsten Erfolge der Strafverfolger in Nordrhein-Westfalen gegen Kinderporno-Ringe wurden ohne das Mittel der Vorratsdatenspeicherung erzielt

Reaktionen

Die vier miteinander verbundenen „Nein, aber"-Urteile des EuGH zur Vorratsspeicherung lösten bei Bürgerrechtlern und Wächtern über die Privatsphäre der Bürger keinen ungetrübten Jubel aus. Der Hamburgische Datenschutzbeauftragte Johannes Caspar etwa erwartet, dass der Richterspruch die Debatte über das Protokollieren von Nutzerspuren neu entfache: „Der EuGH hat den ‚alten Zombie' wieder ins Leben zurückgeholt. Nach jahrelangen Fanfarenstößen für den Datenschutz und die Privatsphäre signalisieren die heutigen Urteile eine zumindest leichte Wendung in der Rechtsprechung des höchsten europäischen Gerichts." Dieses habe sich damit auch den nationalen Diskussionen über die Sicherheit stärker angenähert und seine Gangart aus dem Jahr 2016 gelockert. Er hofft, dass die Gesetzgeber die eröffneten neuen Spielräume allenfalls „mit Augenmaß und Zurückhaltung" nutzten.

Patrick Breyer, EU-Abgeordneter der Piratenpartei, erklärte, die Richter hätten hier „unter dem massiven Druck der Regierungen" und Ermittlungsbehörden „unseren Schutz vor verdachtsloser Kommunikationserfassung" aufgegeben: „Die zugelassene IP-Vorratsdatenspeicherung ermöglicht es, die private Internetnutzung von Normalbürgern auf Monate hinaus zu durchleuchten" und diese gläsern zu machen. Breyer warnte daher davor die Urteile als „Handlungsanweisung" heranzuziehen. Darin beschrieben würden „nur die äußersten Grenzen des rechtlich Machbaren".

Der emeritierte Rechtsprofessor Douwe Korff verwies darauf, dass laut den Entscheidungen Geheimdienste der Mitgliedsstaaten nicht einheitlichen EU-Vorgaben, sondern allein der nationalen Gesetzgebung unterworfen seien. Für sie sei so der Europäische Gerichtshof für Menschenrechte zuständig, demzufolge Maßnahmen wie die Vorratsdatenspeicherung sowie der Zugriff auf Internetknoten im nationalen Ermessen lägen.

Ein breites Bündnis von über 40 zivilgesellschaftlichen Organisationen und Wirtschaftsverbänden aus 16 Ländern hat die EU-Kommission zugleich aufgefordert, anlasslose Telekommunikationsüberwachung im Lichte der Urteile zu verbieten (in diesem Heft, siehe oben S. 236). Friedemann Ebelt von Digitalcourage betonte: „Der Standard in Demokratien muss lauten: keine Vorratsdatenspeicherung."

Die Verlegerverbände VDZ und BDZV sowie der Deutsche Journalisten-Verband (DJV) sehen mit der Weisung aus Luxemburg „die Bürgerrechte ganz grundsätzlich" geschützt. Die für möglich erklärten Ausnahmebestimmungen dürften „nicht zulasten der Presse- und Rundfunkfreiheit gehen". Konstantin von Notz und Tabea Rößner aus der Grünen-Bundestagsfraktion erklärten mit den Urteilen die „pauschale anlasslose Vorratsdatenspeicherung" für „mausetot". Sie seien „eine deutliche Absage" an alle, die sich in den vergangenen Wochen erneut für das Instrument ausgesprochen hätten. Die britische Bürgerrechtsorganisation Privacy International, die zu den Klägern gehört, sieht den Grundsatz der Rechtsstaatlichkeit gestärkt. Demokratien müssten den Überwachungsbefugnissen von Sicherheitsbehörden enge Grenzen setzen (Kuri, Europäischer Gerichtshof: Vorratsdatenspeicherung nein, gezielte Ausnahmen ja, www.heise.de 06.10.2020, Kurzlink: https://heise.de/-4921508; Überwachung: EuGH erlaubt Vorratsdatenspeicherung - aber nur für den Notfall, www.sueddeutsche.de 06.10.2020; Krempl, EuGH-Urteile: Der „alte Zombie" Vorratsdatenspeicherung lebt, www.heise.de 06.10.2020, Kurzlink: https://heise.de/-4922543).

VerfGH Saarland

Gästelistenerhebung ohne gesetzliche Grundlage

Der Verfassungsgerichtshof des Saarlandes (VerfGH) hat mit Beschluss vom 28.08.2020 entschieden, dass eine Verordnung des Saarlandes teilweise gegen die Landesverfassung verstößt, wonach zur Corona-Bekämpfung Gastronomie, Friseure und andere Läden die Kontaktdaten ihrer Kunden sammeln müssen (Az. Lv 15/20).

Die Pflicht zur Erfassung von Gästelisten zur Kontaktnachverfolgung ist ein erheblicher Eingriff in das Grundrecht auf Datenschutz. Diese Pflicht dient der Nachverfolgung und Unterbrechung von Infektionsketten des Coronavirus. Im Saarland ist sie in der „Verordnung zur Bekämpfung der Corona-Pandemie" (CP-VO) geregelt. Ein Rechtsanwalt hatte Verfassungsbeschwerde eingelegt, weil sein Eilantrag beim Verwaltungsgericht gegen die saarländische CP-VO erfolglos geblieben war. Er wehrte sich unter anderem gegen die Verpflichtung zum Tragen einer Maske in verschiedenen Situationen und die Pflicht verschiedener Einrichtungen zur Führung von Gästelisten mit Kundenkotaktdaten.

Im Saarland regelt die CP-VO die Kontaktnachverfolgung. Darin werden Verantwortliche unter anderem von Gastronomie, kulturellen Einrichtungen, Gottesdiensten und Bestattungen, Sport- und sonstigen Veranstaltungen verpflichtet, die Kontaktdaten ihrer Kunden zu erfassen und die Informationen einen Monat lang aufzubewahren. Abgefragt werden müssen Vor- und Familienname, Wohnort, Erreichbarkeit sowie die Ankunftszeit. Auf Anfrage der Gesundheitsbehörde müssen die Betriebe die Daten herausgeben.

Der VerfGH entschied, dass die Bürger die Maskenpflicht hinnehmen müssen. Die Richter wiesen darauf hin, dass seriöse Wissenschaftler sich weitgehend einig darüber sind, dass eine Mund-Nasen-Bedeckung einen, wenn auch kleinen, aber wirkungsvollen Beitrag zur Eindämmung der Pandemie leisten kann. Das sei ein legitimer Zweck. Zum Preis einer bloßen Unannehmlichkeit leiste sie einen Beitrag zur Abwehr von Gefahren für Leben, Gesundheit und

Freiheit aller sowie der Funktionsweise staatlicher und gesellschaftlicher Einrichtungen.

Wegen des Eingriffs in das „Grundrecht auf Datenschutz“ nach Artikel 2 Absatz 2 der Saarländischen Verfassung sieht der VerfGH in der Kontaktnachverfolgung einen erheblichen Eingriff, da Bürger durch die Erfassung, Speicherung und Weitergabe von Adress- und Kontaktdaten mittelbar davon abgehalten werden können, bestimmte Veranstaltungen oder Orte zu besuchen. Für einen derart gravierenden Eingriff bedarf es gemäß dem VerfGH eines Gesetzes. Eine Regierungsverordnung genügt demnach nicht. Da es nicht um eine kurzfristige Notsituation gehe, sondern um eine Regelung, die aller Voraussicht nach länger gelten solle, sei ein parlamentarisches Gesetz erforderlich.

Hierbei handele es sich auch keineswegs um eine „verzichtbare bloße Formalität“. Anders als eine Regierungsverordnung gewährleiste ein parlamentarisches Gesetz die Debatte von Für und Wider vor dem Forum der Öffentlichkeit. Ohnehin sei bei länger dauernden grundrechtlichen Belastungen der parlamentarische Gesetzgeber dafür zuständig, Inhalt und Grenzen der Regelung zu bestimmen.

Weiter rügte das Gericht, dass die Verordnung keine Vorgaben zur Ausgestaltung der Kontaktdatenerhebung mache. Das führe besonders im Bereich der Gastronomie vielfach dazu, dass nachfolgende Gäste wegen der häufig gebräuchlichen „Ringbucherfassung“ erkennen, wer vor ihnen das Unternehmen besucht hat.

Nach Auffassung des Gerichts lässt sich die bei der Kontaktnachverfolgung anfallende Datenverarbeitung nicht auf die Rechtsgrundlage der Einwilligung nach der Datenschutz-Grundverordnung (DSGVO) stützen. Die Freiwilligkeit, eine elementare Voraussetzung der Einwilligung, sei hier nicht gegeben, wenn die Verweigerung der Zustimmung nur für den Preis des weitgehenden Verzichts an der Teilnahme am sozialen Leben möglich sei. Die DSGVO biete auch darüber hinausgehend keine Rechtsgrundlage, sondern nur eine Begrenzung für die Verarbeitung personenbezogener Daten.

Daher kommt der VerfGH zu dem Schluss, dass die Kontaktnachverfolgung ohne gesetzliche Grundlage verfassungswidrig ist. Wegen des „uneingeschränkt legitimen Ziels“ der Kontaktnachverfolgung und weil die bundesweite Rechtsprechung das Problem der fehlenden gesetzlichen Ermächtigungsgrundlage bisher nicht entschieden hat, beschränkte sich das Gericht darauf, eine „Unvereinbarkeitserklärung“ auszusprechen und gab dem saarländischen Landtag bis zum 30.11.2020 Zeit, ein entsprechendes Gesetz zu erlassen. Bis dahin sei es vorübergehend hinnehmbar, dass eine verfassungswidrige Norm in Kraft bleibt (Saarland: Gästelisten sind verfassungswidrig, www.handwerksblatt.de September 2020).

BVerwG

Keine Einwände gegen „Section Control“

Das Bundesverwaltungsgericht (BVerwG) hat den Antrag eines Klägers auf Zulassung der Revision gegen das Urteil des Oberverwaltungsgerichts Lüneburg zurückgewiesen, wonach das bundesweit erste Streckenradar zur Geschwindigkeitskontrolle südlich von Hannover rechtmäßig eingesetzt wird. Damit ist der seit Anfang 2019 laufende Rechtsstreit über Section Control endgültig rechtskräftig abgeschlossen. Für Landesinnenminister Boris Pistorius (SPD) ist das Streckenradar „ein besonderes Anliegen“: „Der Einsatz von Section Control kann einen wesentlichen Beitrag für mehr Verkehrssicherheit leisten.“

Dafür werden an der Bundesstraße 6 bei Laatzen in der Region Hannover Fahrzeuge am Beginn und am Ende eines 2 km langen Messfelds durch eine mit einem Zeitstempel versehene Heckfotoaufnahme (Spurkamera-Foto) erfasst und kurzfristig pseudonymisiert gespeichert. Aus der zwischen den Zeitstempeln liegenden Zeitdifferenz und der Länge des vermessenen Streckenabschnitts wird der Wert der Durchschnittsgeschwindigkeit berechnet. Werktags sind dort täglich mehr als 15.500 Fahrzeuge unterwegs. Ähnliche Anlagen gibt es beispielsweise in Österreich.

Vorteilhaft an dieser Technik sei nach Meinung des Landesinnenministeriums, dass sie für die Verkehrsteilnehmenden gerechter sei, da jede Fahrzeuggeschwindigkeit streckenbezogen gemessen und nur die durchschnittliche Überschreitung verfolgt werde. Dadurch werde gegenüber den punktuellen Blitzern mehr Akzeptanz erreicht. Auch werde der Verkehrsfluss harmonisiert und sicherer.

Wie bei jeder neuen Technik sei auch beim Start von Section Control klar gewesen, dass es einige Hürden geben könne, sagte Pistorius: „Gerade vor diesem Hintergrund bin ich froh, dass wir diesen Schritt als erstes Bundesland seinerzeit gewagt haben.“ Damit könnten auch andere Bundesländer die Technik auf geeigneten Strecken einsetzen. Nach Einschätzung des ADAC gibt es andernorts aber bislang keine konkreten Pläne dafür. Die Anlage sei teurer und aufwendiger als herkömmliche Systeme, daher sei eine Evaluation wünschenswert. Zum Start im November 2019 hatte das Ministerium versichert, wesentliches Ziel der Pilotanlage bleibe „eine umfängliche und wissenschaftliche Beurteilung zur Wirkung der Anlage auf die Verkehrssicherheit.“

Das System war im vergangenen Jahr zeitweise abgeschaltet worden. Ein Anwalt hatte datenschutzrechtliche Bedenken angemeldet. Die Anlage ging wieder in Betrieb, als das niedersächsische Oberverwaltungsgericht die Klage mit Urteil vom 13.11.2019 abwies (12 LC 79/19; Vorinstanz VG Hannover U.v. 12.03.2019 – 7 A 849/19, DANA 2/2019, 110). Hannovers Polizeipräsident Volker Kluwe meinte, nach der Entscheidung des BVerwG sei höchstrichterlich bestätigt, dass es sich beim Streckenradar um ein „modernes und rechtskonformes Mittel der Geschwindigkeitsüberwachung“ handelt.

Angaben des Innenministeriums zufolge wurden von Mitte November 2019 bis Ende Juni 2020 insgesamt 1065 Geschwindigkeitsverstöße von Section Control angezeigt. In 194 Fällen wurden Bußgelder verhängt, in 152 Fällen kamen Punkte für die Fahrer dazu – 17 von ihnen bekamen zusätzlich ein einmonatiges Fahrverbot. Ein Mann fuhr statt der erlaubten 100 Kilometer pro Stunde durchschnittlich 160 (Wilkens, Section Control: Bundesverwaltungsgericht hat keine Einwände gegen Streckenradar,

www.heise.de 28.09.2020, Kurzlink: https://heise.de/-4914143).

BGH

Erben haben vollen Zugriff auf digitalen Nachlass

Der III. Zivilsenat des Bundesgerichtshofs (BGH) hat mit Beschluss vom 27.08.2020 entschieden, dass die Betreiberin eines sozialen Netzwerks, die verurteilt worden ist den Erben einer Netzwerk-Teilnehmerin Zugang zu deren vollständigen Benutzerkonto zu gewähren, den Erben die Möglichkeit einräumen muss vom Konto und dessen Inhalt auf dieselbe Weise Kenntnis zu nehmen und sich – mit Ausnahme einer aktiven Nutzung – darin so „bewegen“ zu können wie zuvor die ursprüngliche Kontoberechtigte (Az. III ZB 30/20).

Facebook war durch ein – vom BGH (U.v. 12.07.2018 – III ZR 183/17, DANA 3/2018, 158 f.) bestätigtes – rechtskräftiges Urteil des Landgerichts (LG) Berlin vom 17.12.2015 verurteilt worden den Eltern einer verstorbenen Teilnehmerin an dem Netzwerk als Erben Zugang zu dem vollständigen Benutzerkonto und den darin vorgehaltenen Kommunikationsinhalten ihrer Tochter zu gewähren (DANA 2/2016, 109 f.). Die Tochter war Ende 2012 in Berlin von einer S-Bahn erfasst und getötet worden. Mit dem Zugriff auf das von Facebook gesperrte Konto wollten die Eltern sich die sie quälende Frage beantworten, ob es sich um einen Unfall oder um Suizid handelte. Facebook hatte nun der Mutter der Verstorbenen einen USB-Stick übermittelt, der eine PDF-Datei mit mehr als 14.000 Seiten enthält, die nach Facebooks Angaben eine Kopie der ausgelesenen Daten aus dem von der Verstorbenen geführten Konto enthält. Diese meinte, dass das soziale Netzwerk damit nicht seiner Verpflichtung auf Zugang zum Account nachgekommen ist, so deren Anwalt Christlieb Klages: „Die PDF-Datei war unübersichtlich und unstrukturiert, durchzogen von Begrifflichkeiten der Programmierung.“ Es habe sich um eine „Secondhand-Datei“ gehandelt, „weil ja nicht das vollständige Konto an die Eltern übergeben, sondern eine Vorauswahl getroffen wurde“. Das Konto selbst war damals in einen sog. „Gedenkzustand“ versetzt worden und somit für einen Zugriff durch Dritte gesperrt.

Das LG hatte daraufhin auf Antrag der Mutter gegen Facebook wegen Nichterfüllung ihrer Verpflichtung aus dem Urteil vom 17.12.2015 ein Zwangsgeld von 10.000 € festgesetzt (B.v. 13.02.2019 – 20 O 172/15). Das Kammergericht (KG) hob den Beschluss des LG auf die sofortige Beschwerde Facebooks auf und wies den Antrag auf Festsetzung des Zwangsmittels zurück (B.v. 03.122019 – 21 W 11/19). Hiergegen hatte sich die vom KG zugelassene Rechtsbeschwerde der Mutter gerichtet. Facebook hatte sich mit dem Argument gewehrt, es wolle das Konto des Mädchens vor einer Nutzung durch die Eltern schützen.

Der BGH hob nun den Beschluss des KG wieder auf und stellte die erstinstanzliche Entscheidung wieder her. Aus dem Urteil des LG Berlin vom 17.12.2015 ging hervor, dass der Mutter nicht nur Zugang zu den im Benutzerkonto vorgehaltenen Kommunikationsinhalten zu gewähren, sondern darüber hinaus auch die Möglichkeit einzuräumen ist vom Benutzerkonto selbst und dessen Inhalt auf dieselbe Art und Weise Kenntnis nehmen zu können, wie es die ursprüngliche Kontoberechtigte konnte. Sowohl das LG wie später der BGH hatten diesen Anspruch der Mutter gegen Facebook erbrechtlich hergeleitet. Der Nutzungsvertrag zwischen der Tochter und Facebook war mit seinen Rechten und Pflichten im Wege der Gesamtrechtsnachfolge auf die Erben übergegangen. Letztere sind hierdurch in das Vertragsverhältnis eingetreten und haben deshalb als Vertragspartner und neue Kontoberechtigte einen Primärleistungsanspruch auf Zugang zu dem Benutzerkonto ihrer Tochter sowie den darin enthaltenen digitalen Inhalten. Aus dieser Stellung der Erben und dem auf sie übergegangenen Hauptleistungsanspruch der Erblasserin aus dem mit Facebook bestehenden Vertragsverhältnis folgt ohne weiteres, dass den Erben auf dieselbe Art und Weise Zugang zu dem Benutzerkonto zu gewähren ist wie zuvor der Tochter. Die „aktive Weiternutzung“ des Profils hat der BGH ausdrücklich ausgeschlossen.

Diesen Pflichten war Facebook nicht nachgekommen. Durch die Überlassung des USB-Sticks mit einer umfangreichen PDF-Datei wurde kein vollständiger Zugang zum Benutzerkonto gewährt. Die PDF-Datei bildet das Benutzerkonto nicht vollständig ab. Letzteres erfordert nicht nur die Darstellung der Inhalte des Kontos, sondern auch die Eröffnung aller seiner Funktionalitäten – mit Aus-

nahme derer, die seine aktive Weiternutzung betreffen – und der deutschen Sprache, in der das Benutzerkonto zu Lebzeiten der Erblasserin vertragsgemäß geführt wurde. Diese Voraussetzungen erfüllt die von der Gläubigerin übermittelte Datei nicht.

Der Klägervertreter Medienanwalt Klages kommentierte: „Es ist eine Entscheidung, die für Tausende Menschen relevant ist, weil sie die Frage behandelt, wie ich als Erbe später einmal Einsicht nehmen kann in die Unterlagen des Erblassers" (BGH, PM Nr. 119 v 09.09.2020, Zur Auslegung eines Urteils, das die Betreiberin eines sozialen Netzwerks verpflichtet, den Erben der Berechtigten eines Benutzerkontos Zugang zum vollständigen Konto zu gewähren; Barisic, 14000 Seiten PDF sind zu wenig, SZ 10.09.2020, 8).

LAG Niedersachsen

Auskunftsanspruch erstreckt sich nicht auf alle Beschäftigten-E-Mails

Mit Urteil vom 09.06.2020 hat das Landesarbeitsgericht Niedersachsen (LAG) entschieden, dass ein ehemaliger Beschäftigter keinen Anspruch darauf hat Kopien sämtlicher E-Mails zu verlangen, die er während seiner beruflichen Tätigkeit verfasst hatte (Az. 9 Sa 608/19). Gemäß Art. 15 DSGVO sind Arbeitgeber verpflichtet auf Antrag von gegenwärtigen oder ehemaligen Beschäftigten innerhalb eines Monats (vollständige) Auskünfte über die im Arbeitsverhältnis verarbeiteten personenbezogenen Daten zu gewähren.

Nach Auffassung des LAG sind von dem Auskunftsanspruch gemäß Art. 15 DSGVO jedoch nicht die eigenen E-Mails des ehemaligen Beschäftigten umfasst, da diese dem Beschäftigten bereits bekannt sind:

„Dem Kläger ist der E-Mail-Verkehr, den er selbst geführt oder erhalten hat, bekannt, sodass es nach dem Schutzzweck keinen Anlass gibt, diesen gesamten E-Mail-Verkehr zur Verfügung zu stellen. Sinn und Zweck der Auskunftserteilung und Zurverfügungstellung einer Kopie ist es, den betroffenen Personen eine Überprüfung der Datenverarbeitung zu ermöglichen, nicht aber vollständige Kopien aller Unterlagen zu erhalten, in denen personenbezogene Daten über sie enthalten sind".

In der obergerichtlichen Rechtsprechung wird der Umfang des Auskunftsanspruchs nach Art. 15 DSGVO unterschiedlich beurteilt. So geht z.B. das Oberlandesgericht Köln davon aus, dass unter die Vorschrift „sowohl im Kontext verwendete persönliche Informationen wie Identifikationsmerkmale (z.B. Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht, Augenfarbe, Größe und Gewicht) oder innere Zustände (z.B. Meinungen, Motive, Wünsche, Überzeugungen und Werturteile), als auch sachliche Informationen wie etwa Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt" fallen (LAG Niedersachsen: Auskunftsanspruch nach DSGVO erfasst nicht E-Mails des ehemaligen Beschäftigten, www.anwalt.de 22.10.2020).

LAG Berlin-Brandenburg

Arbeitszeitnachweis per Fingerabdruckscanner bleibt freiwillig

Das Landesarbeitsgericht Berlin-Brandenburg (LAG) hat mit Urteil vom 04.06.2020 auf die Klage eines medizinisch-technischen Assistenten hin entschieden, dass dieser vom Arbeitgeber, einer radiologischen Praxis, nicht verpflichtet werden kann, seine Arbeitszeit mit seinem Fingerabdruck nachzuweisen (Az.: 10 Sa 2130/19). Eine Revision zum Bundesarbeitsgericht (BAG) wurde nicht zugelassen.

Die Erfassung biometrischer Daten sei in dem Fall nicht ohne Einwilligung des Arbeitnehmers zulässig. Eine Verarbeitung solcher Daten sei nach der Datenschutz-Grundverordnung nur ausnahmsweise möglich. Das System, das zum Einsatz kommen sollte, erfasst den Fingerabdruck nicht als Ganzes, sondern Fingerlinienverzweigungen. Der Assistent hatte diese Erfassung abgelehnt und eine Abmahnung des Arbeitgebers kassiert, wogegen er vor Gericht zog.

Auch wenn das System nur Fingerlinienverzweigungen verarbeitet, handele es sich, so das Gericht, um biometrische Daten. Es konnte in dem Fall nicht feststellen, dass eine solche Erfassung erforderlich ist. Die Weigerung des Assistenten ist daher keine Pflichtverletzung. Er kann verlangen, dass die Abmahnung aus der Personalakte entfernt wird (Költzsch, Arbeitnehmer müssen Fingerabdruck nicht bereitstellen, www.golem.de 25.08.2020).

LG Dresden

Anspruch auf unentgeltliche Auskunft über Krankenhausbehandlung

Das Landgericht Dresden (LG) hat mit Urteil vom 29.05.2020 entschieden, dass Patienten von einem Krankenhaus die kostenlose Herausgabe ihrer abgespeicherten personenbezogenen Daten verlangen können, wobei es nicht darauf ankommt, für welche Zwecke die Patienten sie benötigen (Az.: 0 76/20). In dem Fall forderte eine Frau unter Bezugnahme auf die Datenschutz-Grundverordnung (DSGVO) von einer Klinik unentgeltlich Auskunft über ihre personenbezogenen Daten und damit auch ihre Behandlung, die nach ihrer Ansicht fehlerhaft gewesen ist. Die Klinik hatte eine Zusendung ohne Kostenübernahmeerklärung abgelehnt. Dabei ging es um eine Summe von knapp sechs Euro für einen USB-Stick und die anfallenden Portokosten. Die Frau beharrte mit Erfolg darauf, dass die Klinik ihr die vollständige Dokumentation der Behandlung als PDF-Dokument unentgeltlich zukommen lässt.

Das LG entschied, die Klägerin habe Anspruch auf die kostenlose Übermittlung der Daten. Die Speicherung gesundheitsbezogener Daten falle in den Anwendungsbereich der DSGVO. Die Klinik könne die Zusendung dieser Daten nicht von der Übernahme der Kosten abhängig machen. Die erstmalige Herausgabe müsse kostenlos erfolgen und die Unterlagen – sofern gewünscht – in einem elektronischen Format übermittelt werden. Keine Rolle spiele dabei, für welchen Zweck der datenschutzrechtliche Auskunftsanspruch erhoben werde (Krankenhaus muss Patientin kostenlos Daten übermitteln, www.rheinpfalz.de 22.09.2020).

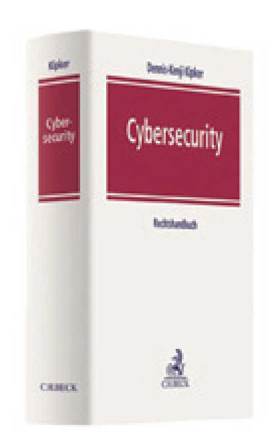
Buchbesprechungen



Kugelmann, Prof. Dr. Dieter (Hrsg.)
Landesdatenschutzgesetz Rheinland-Pfalz – Handkommentar
1. Auflage 2020, 608 Seiten,
ISBN 978-3-8487-5428-1, 98,- €

(wh) Der seit dem 01. Oktober 2015 amtierende Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz hat als Herausgeber eine illustre Schar renommierter AutorInnen versammelt, die diesen Handkommentar erstellt haben. Eines der wesentlichen Ziele dieses Kommentars sei es, schreibt Kugelmann in seinem Vorwort, „die Regeln des Landesdatenschutzgesetzes zu erläutern, indem ihre Zusammenhänge [mit der DSGVO und der JI-Richtlinie] verdeutlicht werden." Kugelmann stellt in seiner Kommentierung des § 1 des Landesdatenschutzgesetzes Rheinland-Pfalz (LDSG-RP) die Zusammenhänge des LDSG-RP nicht nur mit der DSGVO und der JI-Richtlinie dar, sondern ordnet es auch tiefergehend in die Kombination aus Grundrechten aus dem Grundgesetz, der Rheinland-Pfälzischen Verfassung und den Art. 7 und 8 der Europäischen Grundrechtecharta ein. Nicht unerwähnt lässt Kugelmann die Tatsache, dass Rheinland-Pfalz als drittes Land bereits 1974 nach Hessen (1970, nachträglich herzlichen Glückwunsch zum 50. Geburtstag) und Schweden (1973) ein Datenschutzgesetz erließ. Wichtig ist auch die Einordnung des LDSG RP zwischen DSGVO und bereichsspezifischen Datenschutzregelungen („lex specialis"). Der Anwendungsvorrang der DSGVO wird ausführlich erörtert und am Beispiel des § 4 BDSG „Videoüberwachung öffentlich zugänglicher Räume" dargestellt. Mit der Begründung des BVerwG, das die Anwendbarkeit des § 4 BDSG für nichtöffentliche Stellen verneint hat, sieht Kugelmann auch die Nichtanwendbarkeit der entsprechenden Regelung aus § 21 Abs. 1 Satz 2 gegeben. Der Kommentator dieses Paragraphen formuliert es hier etwas vorsichtiger, er schreibt von Zweifeln an der Vereinbarkeit dieser Regelung mit dem Europarecht.

Die Kommentierung kann als gelungen bezeichnet werden. Die hergestellten europarechtlichen Bezüge sowie die Verweise auf das Bundesdatenschutzgesetz und auf Vorgängerregelungen in Rheinland-Pfalz sind bei der Interpretation des aktuellen LDSG-RP sehr hilfreich. Ein ausführliches Stichwortverzeichnis rundet das Werk ab, so dass der Autor dieser Rezension dieses Werk all denen empfehlen kann, die sich mit dem rheinland-pfälzischen Datenschutzrecht beschäftigen wollen oder müssen.



Dennis-Kenji Kipker (Hrsg.)
Cybersecurity – Rechtshandbuch
1. Auflage 2020, 597 Seiten,
ISBN 978-3-406-73011-5, 119,– €

(rz) Das Buch „Cybersecurity" ist ein in jeder Hinsicht beachtliches Werk zur Cyber-Sicherheit.

Cyber-Sicherheit, als Oberbegriff zu den Themenfeldern Datensicherheit, Datenschutz, IT- und Informationssicherheit, hat im Hinblick auf die großen IT-Sicherheitsvorfälle der letzten Jahre erheblich an Bedeutung gewonnen. Dieses umfassende Werk gibt der spannenden und bisher unzureichend betrachteten Gemengelage zwischen Datenschutzrecht, IT-Sicherheitsrecht und Informationssicherheitsrecht dabei zunächst eine Struktur. Der Leser erhält einen umfassenden und leicht nachvollziehbaren Überblick über die einzelnen Themenbereiche und deren Beziehungen zueinander.

Besonders hervorzuheben sind dabei die technischen Erläuterungen. So sind gerade die Erläuterungen der technischen Grundlagen der Informationssicherheit von besonderem praktischen Nutzen und auch für Nicht-Techniker sehr gut nachvollziehbar.

Für Datenschützer von besonderem Interesse dürfte – neben den Ausführungen zum Datenschutz selbst – in diesem Zusammenhang besonders auch das Kapitel zum „Stand der Technik" sein.

Unter rechtlichen Aspekten werden alle relevanten Rechtsbereiche mit Bezug zur Cyber-Sicherheit dargestellt, wie bspw. das IT-Vertragsrecht, das zivile Haftungsrecht, das Arbeitsrecht und die verschiedenen Aspekte des IP- und Wettbewerbsrechts. Abgerundet wird dies durch die Darstellungen internationaler Rahmenvorgaben einschließlich des Völkerrechts.

Bemerkenswert ist dabei der stets sehr hohe Praxisbezug. So wird in weiteren Kapiteln auf die Verantwortlichkeit, die Implementierung und die Corporate Governance rund um das Thema Cyber-Sicherheit eingegangen. Auch finden sich branchenübergreifende Vorgaben zur IT-Sicherheit und spezifische Sonderkonstellationen wie das Cloud Computing oder BYOD. In eigenen Kapiteln werden die prozessuale Durchsetzung sowie die Themen Gefahrenabwehr und Sanktionierung dargestellt.

Darüber hinaus wird durch eine besondere Betrachtung und Einordnung von kritischen Infrastrukturen und ein Kapitel zum Recht der Nachrichtendienste im Ergebnis den meisten Lesern ein noch nie dagewesenes Gesamtbild der Cyber-Sicherheit geboten.

Fazit: Mit diesem Werk tritt das Recht der Cyber-Sicherheit nun endgültig aus dem Schatten des Datenschutzrechts heraus, wo es bisher meist nur als „technisches Anhängsel" betrachtet wurde. Dort wo der Datenschutz auf die technischen und organisatorischen Maßnahmen trifft, setzt dieses Buch mit seinem 360 Grad Blick auf die durchaus komplexe Schnittmenge zwischen Datenschutz, Informationssicherheit und IT-Sicherheit neue Maßstäbe. Es handelt sich damit um ein Grundlagen- und Standardwerk, das jedem Studenten, Praktiker und Akademiker, der sich mit dem Thema Datenschutz, Informationssicherheit oder IT-Sicherheit befasst, dringend ans Herz gelegt werden muss.



RA Dr. Florian Sackmann
Datenschutz bei der Digitalisierung der Mobilität – Eine sektorspezifische Analyse der Leistungsfähigkeit und des Weiterentwicklungsbedarfs der Datenschutzordnung, 1. Auflage 2020, 211 Seiten, ISBN 978-3-8487-6652-9 (Softcover), ISBN 978-3-7489-0731-2 (eBook), je 54,- € – Dieses Werk ist Band 43 der „Reihe Recht der Informationsgesellschaft", die seit Band 34 im Nomos-Verlag erscheint.

(wh) Das Werk wurde als Dissertation an der Universität Regensburg angenommen und ist entsprechend wissenschaftlich gestaltet. Üblicherweise erwartet der Autor dieser Rezension im Vorwort ein paar Sätze zum Ziel oder Inhalt des Werkes, hier sind es nur Danksagungen. Aber ein Blick auf die entsprechende Webseite des Verlags hilft hier weiter. Die Ziele der Arbeit sind: „in einer Realweltanalyse die besonderen Herausforderungen für den Schutz der Privatsphäre, die sich durch eine datengetriebene Mobilität stellen" zu identifizieren, „auf der Basis des geltenden Rechts" Lösungsmöglichkeiten zu entwickeln und Defizite des geltenden Datenschutzrechts herauszuarbeiten. „Daraus wird schließlich der aktuelle legislative Handlungsbedarf ermittelt."

Zu Beginn werden insbesondere die Begriffe Digitalisierung und Mobilität in ihrer im Werk verwendeten Bedeutung herausgearbeitet. Deutlich wird hier, dass in der Arbeit – verständlicherweise – „die Mobilität im Sinne des Personenverkehrs untersucht" wird. Hier ist der Personenbezug im Zusammenhang mit der Mobilität am größten. Betrachtet werden in Fallstudien die drei Bereiche „Der individuelle Straßenverkehr", „Digitale Dienste im öffentlichen Personenverkehr" und „Digitale Dienste im Luftverkehr". Dabei wird im ersten Bereich zwar auf Mitfahrzentralen und das sogenannte „free floating carsharing" eingegangen, nicht aber auf datenschutzrechtliche Fragestellungen, die sich bei der Nutzung von Mietwagen ergeben. Im anschließenden Abschnitt erfolgt eine Einordnung des EU-Datenschutzrechts, selbstverständlich unter Erwähnung der Art. 7 und 8 der Europäischen Grundrechtecharta. Die Anwendbarkeit von EU-Datenschutzrecht, BDSG und Landesdatenschutzgesetzen – letzteres im Bereich des ÖPNV – wird als Problem dargestellt. Der Autor sieht trotz der DSGVO eine zu große Heterogenität des EU-Datenschutzrechts, die sich seiner Auffassung nach als „entwicklungshemmend" erweist. Die Fragestellungen, welche der anfallenden Mobilitätsdaten personenbezogene Daten sind und wer für diese Daten der Verantwortliche im Sinne der DSGVO ist, werden ausführlich erörtert. Beruhigend ist, dass der Autor der Ansicht ist, „dass die sich stellenden Probleme durch das gegenwärtige Recht lösbar sind", auch wenn „Rechtsunsicherheit und Bürokratie [...] die Kerndefizite der Datenschutzordnung für den Mobilitätssektor" seien. Die folgenden Lösungsansätze sind interessant und diskussionswürdig.

Zwar gibt es ein ausführliches Literaturverzeichnis, aber ein Stichwortverzeichnis fehlt leider. Trotz dieses Mangels gibt dieses Werk einen guten und umfassenden Überblick zu den datenschutzrechtlichen Herausforderungen, die sich durch die Digitalisierung der Mobilität ergeben. Durch die dargestellten Lösungsansätze werden zudem Möglichkeiten gezeigt, wie diesen Herausforderungen zumindest datenschutzrechtlich begegnet werden kann.



Bergmann, Lutz (verst.)/
Möhrle, Roland/Herb, Armin
Datenschutzrecht
Boorberg Stuttgart
60. Ergänzungslieferung, August 2020

(tw) Die Besprechung von Loseblattsammlungen ist immer mit einer gewissen Ungewissheit verbunden: Es ändert sich regelmäßig nicht nur das Recht, sondern auch der Inhalt. Es lohnt sich, Aktualisierungen vorzunehmen, selbst wenn diese nur einen Zwischenstand wiedergeben. Das gilt insbesondere für den Bergmann/Möhrle/Herb, zitiert oft abgekürzt mit „BMH". Es handelt sich dabei wohl um die meistzitierte und bestsortierte Loseblattsammlung zum deutschen Datenschutzrecht, die aber mit den schnell folgenden Neuauflagen der gebundenen Kommentierungen zu der DSGVO und zum BDSG nicht Schritt halten kann. Dennoch: Der BMH holt auf (vgl. DANA 3/2017, 179). Die 60. Ergänzungslieferung überholt sogar vereinzelt andere Grundsatzwerke, indem sie z.B. das neu 2020 verabschiedete „Datenschutz-Grundverordnungs-Aus-

füllungsgesetz Sachsen-Anhalt" dokumentiert. Waren die Landesgesetze in den Frühzeiten des Datenschutzes die Trendsetter des Rechtsgebiets, so sind sie inzwischen weitergehend verdrängt und erfüllen nur Lücken-Ausfüllungsfunktion. Im öffentlichen Bereich bleiben sie aber weiterhin von Relevanz; insofern ist der Zugriff auf sie wichtig, der durch den BMH aktuell bzgl. aller Länder gewährleistet wird. Entsprechendes gilt für die Kirchengesetze.

Ein früher Vorteil des BMH bestand darin, dass wichtige bereichsspezifische Regelungen dokumentiert und kommentiert wurden. Diesen Vorteil aufrecht zu erhalten, schaffen die neuen Ausgaben des BMH nicht mehr. Das Telekommunikations- und Medienrecht ist in einem Umbruch, ebenso das Sozialrecht, das vorläufig ganz aus dem BMH verschwunden ist; beim Bundesmeldegesetz bleibt es weitgehend beim Abdruck des Gesetzes. Die Ausdifferenzierung des spezifischen Datenschutzrechts setzt hier Grenzen.

Im Vordergrund steht aber natürlich die DSGVO. Und hier erreicht der BMH inzwischen einen Umfang, der es erlaubt, ihn auch bei Spezialfragen zu Rate zu ziehen, ohne Gefahr zu laufen, auf eine Lücke zu stoßen. Die aktuelle Ergänzungslieferung liefert Kommentare zu den Art. 37-43, 50, 53, 54, 69-76, 81-88. Damit fehlen nur noch wenige Regelungen, nämlich die Art. 46-49, 52, 55-57, 62-67 – alles Normen, die in der praktischen Anwendung eher nicht im Fokus stehen. Förderlich bei den Kommentierungen ist, dass diese zurückgreifen auf die gebundenen Kommentare und damit einen kurzen Überblick über den Diskussionsstand zu einzelnen Normen geben. Inhaltlich bewegen sich die Ausführungen auf einem guten Niveau. Zugleich ist aber festzustellen, dass die Kommentierungen oft an der Oberfläche bleiben und kurz geraten sind. Der BMH zum alten BDSG zeichnete sich dadurch aus, dass in Ergänzungslieferungen zunächst rudimentäre Erläuterungen durch sehr tief gehende ersetzt wurden. Insofern besteht, nachdem Vollständigkeit erreicht wird, Luft nach oben. Für den schnellen Überblick und das Nachschlagen zu speziellen Fragen ist der BMH heute wieder eine wichtige Hilfe.

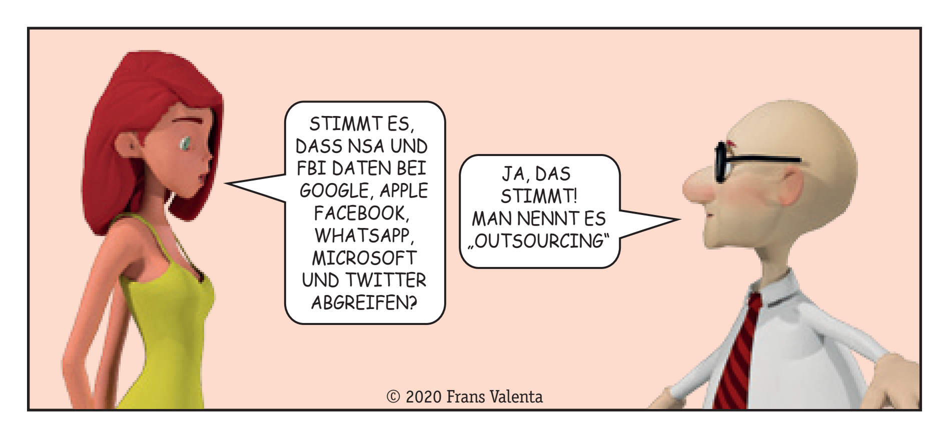


Dr. Martin Zilkens
und Dr. Lutz Gollan (Hrsg.)
Datenschutz in der Kommunalverwaltung – Recht – Technik – Organisation
5. Auflage 2019, 785 Seiten, ISBN 978-3-503-18758-4, 108,- €

(wh) Sich mit dem Datenschutz in der Kommunalverwaltung zu beschäftigen ist aufgrund der föderalen Struktur Deutschlands eine herausfordernde Aufgabe. Schließlich gilt für die Kommunen ergänzend zur EU-Datenschutz-Grundverordnung (DSGVO) und bereichsspezifischen Gesetzen auf Bundes- und Länderebene das jeweilige Landesdatenschutzgesetz. Hierzu ist allerdings festzustellen, dass in diesem Werk auf Landesebene in erster Linie das nordrhein-westfälische Recht beispielhaft berücksichtigt wird. Dies ist vermutlich auch der Tatsache geschuldet, dass die Hälfte der AutorInnen in Nordrhein-Westfalen tätig ist. Insoweit ist es vorteilhaft, dass ein Teil der landesrechtlichen Datenschutzregelungen durch die DSGVO ersetzt wurde und im Bereich der Anwendbarkeit der DSGVO nun für alle Bundesländer grundsätzlich einheitliche Regelungen gelten. Einer der Herausgeber sieht es dagegen seit dem Gültigwerden der DSGVO als schwieriger als vorher an, die jeweils anzuwendende Datenschutzvorschrift herauszufinden. Dies wird mit Ausnahmen und Gegenausnahmen begründet, so als ob es diese im Datenschutzrecht nicht auch schon bereits vor der DSGVO gegeben hätte.

Nach einer umfassenden Darlegung der Grundlagen des Datenschutzrechts werden im Kapitel „7 Bereichspezifischer Datenschutz" die datenschutzrechtlichen Besonderheiten der wesentlichen Bereiche der Kommunalverwaltung erörtert. Dem Beschäftigtendatenschutz wird ebenso wie dem „Datenschutz bei kommunalen Belangen" jeweils ein eigenes ausführliches Kapitel gewidmet. Kapitel zur „Datenschutzkontrolle und Aufsicht", zu Dienst- und Geschäftsanweisungen sowie zum technischen Datenschutz runden das Werk ab. Ein Kapitel über das „öffentliche Informationszugangsrecht" schließt dieses Werk ab. Dabei ist es wenig verwunderlich, dass hier nicht auf die in den verschiedenen Bundesländern geltenden Regelungen eingegangen werden kann, denn dies würde ein eigenständiges umfangreiches Werk erfordern. Am Beispiel der nordrhein-westfälischen Regelungen wird das Zusammenspiel zwischen den Regelungen zu Informationsfreiheit auf Bundes- und Landesebene anschaulich dargestellt. Dieses Werk ist im Bereich des kommunalen Datenschutzes eine hilfreiche Ergänzung zu einem Kommentar des in der Kommune geltenden Landesdatenschutzgesetzes.

Cartoon





https://www.heise.de/news/Terrorbekaempfung-und-Verschluesselung-EU-Rat-forciert-umstrittene-Crypto-Linie-4960069.html